



12 Дмитрий ФРОЛОВ
(Банк России)
**Кибербезопасность
финрынка: первый годовой
отчет FinCERT**

28 Александр БОДРИК
(эксперт)
**Есть проблема! И не будем
этого скрывать!**

36 Александр БАБКИН
(Газпромбанк)
СОС: Три ноу-хау Газпромбанка

90 Артем ЗУБКОВ
(издатель)
Игра на опережение



94 Сергей ЛЕБЕДЬ
(Сбербанк)
Готовим кибердружину!

СОС В БАНКЕ. ВЫБИРАЙ ЛЮБОЙ!



АВАНГАРД

медиа группа



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Книжное
издательство

ib-bank.ru
kzi.su

soc-forum.ib-bank.ru
pki-forum.ru

inkas.ib-bank.ru
ctcrypt.ru



Павел БЫЛЕВСКИЙ

шеф-редактор
BIS Journal

В отечественной отрасли информационной безопасности в последнее время наблюдаются тектонические сдвиги. Спринтерскими темпами развивается нормативно-правовая база (включая «закон Яровой»). Создаются структуры качественно нового уровня (ГосСОПКА, подобные ведомственные, отраслевые, корпоративные формирования). Небывальными прежде темпами развивается такое взаимодействие государственных органов, о каком прежде лишь мечталось. И, что очень важно — наблюдается мобилизация профессионального сознания специалистов по информационной безопасности, — в смысле военном, а не умелого использования гаджетов.

Все эти перемены происходят и у нас, в кредитно-финансовой сфере. Это один из передовых рубежей обороны, наряду с фронтами «незримых боев». Атаки злоумышленников на кредитно-финансовые организации, клиентские сервисы напрямую наносят урон российским компаниям и гражданам. Результаты этих атак почти невозможно скрыть, они сразу становятся широко известными, наносят не только заметный финансовый, но и моральный ущерб.

Злоумышленников привлекают и химеры быстрого криминального обогащения, и бандитский кураж вседозволенности, безграничной власти «сверхчеловека» над денежными средствами «тварей дрожащих». Пока остаётся открытым вопрос, не являются ли атаки «анонимных хакеров» на интернет-ресурсы российских государственных регуляторов и крупнейших системообразующих банков элементом необъявленных, тайных «гибридных» войн. Но скоро это перестанет быть тайной, и это вопрос не столь отдалённого времени.

К счастью, мы живём во время не только катастрофического нарастания информационных угроз, набирающего мощь киберкриминалитета, усложнения и усиления его инструментария. В то же время мы с удовлетворением видим слаженную работу коллег по выстраиванию новых и новых рубежей обороны, накопление резервов для контратак, нацеленность на то, чтобы впоследствии разгромить неприятеля в его логове.

Одним из важнейших направлений вывода информационной безопасности отрасли на качественно новый уровень является автоматизация, создание и выстраивание взаимодействия SOC'ов — FinCERT Банка России, крупных банков, а также корпоративных, оказывающих услуги на аутсорсинге. Именно этой главной теме и посвящены статьи этого номера нашего журнала. Представители государственных органов, банков, кредитно-финансовых организаций, эксперты информационной безопасности делятся самым актуальным опытом, формулируют проблемы и предлагают пути их решения. Пусть эта дискуссия послужит вкладом в общее дело.

... Недавние голословные обвинения России в кибератаках со стороны вице-президента США Джозефа Байдена, угрозы встречных мер и финансовых санкций только подтверждают правильность нашей работы.

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

Емельянов Г.В. — член-корреспондент Академии криптографии РФ, действительный государственный советник РФ 3 класса
Сычев А.М. — заместитель начальника Главного управления безопасности и защиты информации Банка России, кандидат технических наук, доцент
Шипилов В.В. — исполнительный директор Ассоциации российских банков, кандидат технических наук

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Былевский П.Г. — шеф-редактор, кандидат философских наук
Велигура А.Н. — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПС», CISA, кандидат физико-математических наук
Виноградов А.Ю. — начальник управления информационной безопасности АО КБ «Златкомбанк»
Вихорев С.В. — директор по информационной безопасности Филиала «ПЕТЕР-СЕРВИС Спецтехнологии»
Держинский Ф.Я. — главный эксперт — координатор системной экспертизы блока «информационные технологии» департамента информационных технологий ОАО «Промсвязьбанк», CSDP
Зубков А.Н. — генеральный директор ООО «Медиа Группа „Авангард“»
Курило А.П. — руководитель по направлению информационной безопасности в финансовом секторе компании INLINE Technologies, кандидат технических наук
Левиев Д.О. — председатель Совета НП «Партнерство специалистов по информационной безопасности»
Мельников С.Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», кандидат физико-математических наук
Некрасов И.В. — главный редактор журнала
Окулесский В.А. — начальник управления безопасности АО «Национальная система платёжных карт», кандидат технических наук
Паизин С.В. — начальник Управления по обеспечению информационной безопасности ОАО Банк ВТБ, кандидат физико-математических наук
Шумский Л.С. — начальник Управления контроля информационных рисков, ДОР (АО) Связной Логистика
Янсон И.А. — бизнес-партнер по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

ЭКСПЕРТНАЯ ГРУППА

Одувалов М.В. — эксперт BIS Journal
Филипчук А.А. — вице-президент АБ «ГПБ-ипотека» (группа «Газпромбанка»)

РЕДАКЦИЯ ЖУРНАЛА

Шеф-редактор: **Былевский П.Г.**
Главный редактор: **Некрасов И.В.**
Директор по развитию: **Минаков А.В.**
Дизайн-макет: **Раснюк А.С.**
Обозреватели, корреспонденты: **Бендин С.В., Коротышев П.Г., Северный В.П., Хвастунова О.Н.**
Иллюстрация на 1-й обложке: **Ларичкина О.А.**
Фото в номере: **фотобанк Shutterstock**
Верстка: **Мельников Н.С.**
Цветокорректор: **Науменко М.Б.**
Корректор: **Бальтерманц Л.Ф.**
Выпускающий редактор: **Богданов А.Д.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группа „Авангард“»
Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д.21 (м. «Достоевская»)
Координаты: 55.779380, 37.61150
Тел./факс: +7 499 271-70-85
Интернет-версия: journalib-bank.ru
E-mail: bis@ib-bank.ru
Отдел рекламы: reklama@ib-bank.ru
Отдел распространения: tirazh@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).
Свидетельство ПИ № ФС77-55062 от 14 августа 2013 г.
Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal — Информационная безопасность банков».

Перепечатка и воспроизведение иными способами без разрешения редакции запрещаются.
При использовании материалов ссылка на журнал обязательна.
Мнение редакции может не совпадать с мнением авторов.
Присланные материалы не рецензируются и не возвращаются.

Подписан в печать 17.10.2016. Тираж 7000 экз.
Заказ № 945/5. Цена договорная.
Отпечатан в «Типографии на Угрешской»
115088 РФ, Москва, ул. Угрешская, д.2, стр.2.
Тел. +7 495 720-62-28

© BIS Journal, 2016

НОВОСТИ

5 Угрозы и решения

РЕГУЛЯТОРЫ

8 Стандартизация / Александр ВИНОГРАДОВ (АО КБ «Златкомбанк»), **Фарит МУЗИПОВ** (ООО КБ «АйМаниБанк»), **Владимир ГОЛОВАНОВ** (ООО НПФ «Кристалл») **СТО БР ИББС. По случаю юбилея**

12 FinCERT / Дмитрий ФРОЛОВ (Банк России) **Кибербезопасность финрынка**

18 Аутсорсинг / Артем СЫЧЕВ (Банк России), **Сергей ВИХОРЕВ** (ПЕТЕР-СЕРВИС Спецтехнологии) **Поговорим об аутсорсинге безопасности информации**

БАНКИ

28 SOC / Александр БОДРИК (эксперт ИБ) **SOC'и России. Есть проблемы. И не будем этого скрывать!**

36 Александр БАБКИН (Газпромбанк) **Три ноу-хау Александра Бабкина**

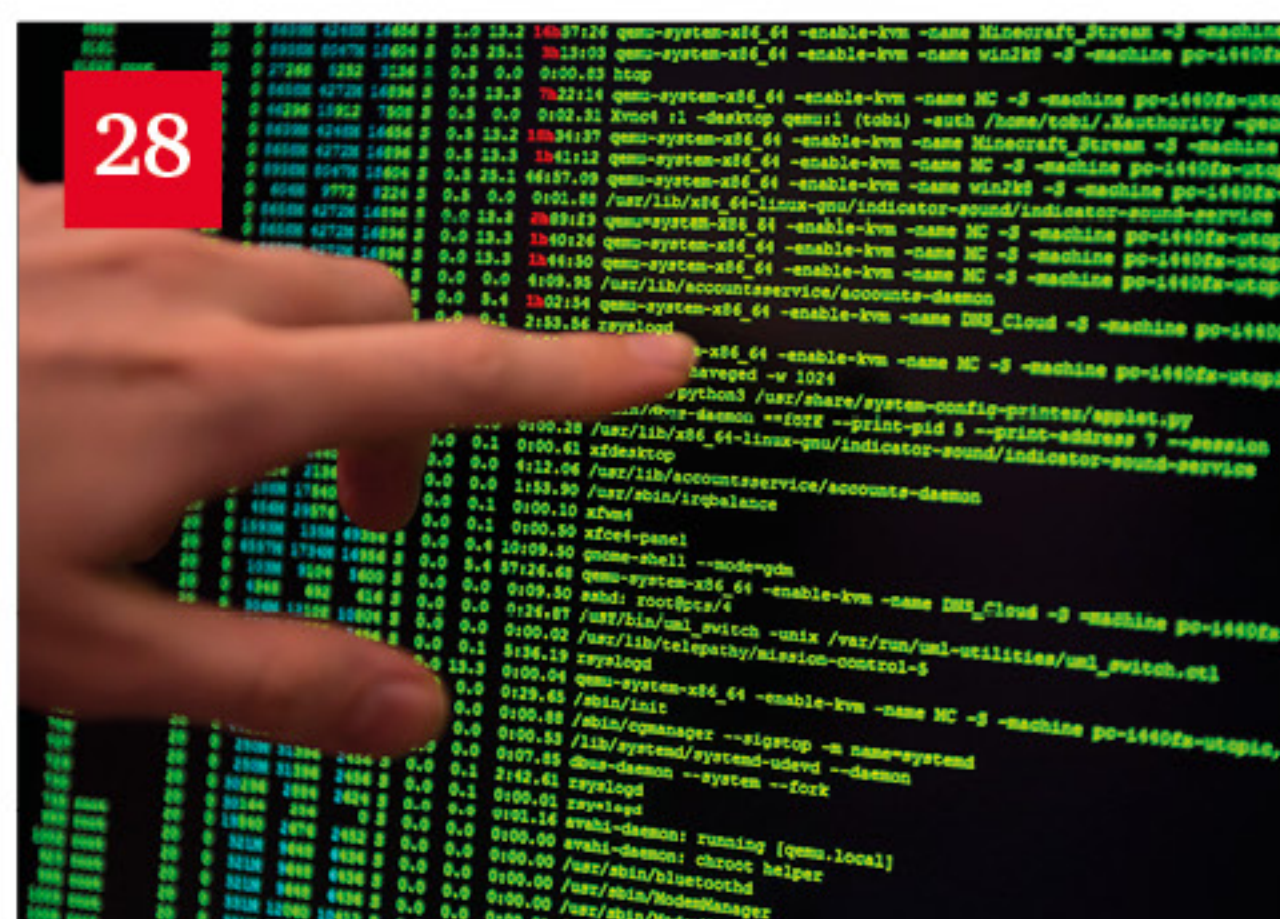
42 Сергей ЗИНОВКИН, Игорь АГУРЬЯНОВ (Сбербанк) **Эффективная DLP в эпоху перемен**

46 Андрей ЯНКИН (Инфосистемы Джет) **SOC 2.0. Аппетит приходит во время еды**

48 Алексей МАЛЬНЕВ (АМТ-ГРУП) **Подбирая лучшее для SOC**

50 Криптовалюты / Денис ДЫГИН, Иван ЛАВРИКОВ, Григорий МАРШАЛКО, Василий ШИШКИН (ТК 26) **Электронные валюты: технические и нормативные вопросы функционирования и обеспечения безопасности**

53 Алексей АРХИПОВ, Константин КОЛЬЦОВ (QIWI) **Блокчейн — начало пути**



62



67



82



86



УГРОЗЫ И РЕШЕНИЯ

- 54** За рубежом / Юрий ЩЕРБАКОВ
(эксперт ИБ)
Секреты вредоносного кода
- 60** Инциденты / Михаил БОГАТЫРЁВ,
Сергей НЕЙГЕР
(Перспективный мониторинг)
Дело не на одну пиццу
- 62** Биометрия / Константин СИМОНЧИК
(ООО «Центр Речевых
Технологий»), Дмитрий ЩЕТИНИН
(ООО «ЦРТ-инновации»)
Защита от подделки голоса
в биометрических системах:
современное состояние дел
- 67** Экспертиза проблемы / Константин СМЕРНОВ,
Артём АГЕЕВ (Accenture)
Два берега И-реки
- 72** Осторожно, инсайдер! / Алексей БАБЕНКО
(Информзащита)
Как найти волка в овечьей шкуре, или
выявляем внутреннее мошенничество
- 74** Управление безопасностью / Денис СУХОВЕЙ
(Аладдин Р.Д.)
Течёт! Пять явных признаков
утечки информации в организации
- 76** SIEM / Владимир БЕНГИН
(Positive Technologies)
С SIEM`ом или на щите:
банковская специфика
- 78** Мария ЛУРЬЕ (С-Терра СиЭсПи)
Сказки-ПодСказки от С-Терра

ИНФРАСТРУКТУРА

- 82** Деловые мероприятия / Андрей КУРИЛО
(НП НСФР)
Обострение практикой
- 86** Электронный документооборот / Нина СОЛОВЯНЕНКО
(Институт государства и права РАН)
Каким может быть закон об электронном
документе

ИНфраСТРУКТУРА

- 88** **Деловые мероприятия**
InfoSecurity Russia 2016. Меньше, да лучше
- 90** **Образование и карьера / Артем ЗУБКОВ**
(Медиа Группа «Авангард»)
Игра на опережение
- 92** **Владимир НИКОНОВ**
(Академия криптографии РФ)
Логика победы
- 94** **Сергей ЛЕБЕДЬ** (Сбербанк)
Готовим кибердружину!
- 96** **Марина БРОДСКАЯ** (BIS Journal)
Много лифтов на Олимп

СУБЪЕКТЫ

- 98** **Молодой специалист / Марина БРОДСКАЯ**
(BIS Journal)
Не просто Мария
- 102** **Корифеи / Геннадий ЕМЕЛЬЯНОВ**
(Академия Криптографии РФ),
Дмитрий ЛАРИН (кандидат
технических наук)
Они ковали Победу
- 110** **Мысли вслух / Сергей ВИХОРОВ**
(ПЕТЕР-СЕРВИС Спецтехнологии)
Меня терзают смутные сомнения...
- 113** **Александр БОДРИК** (эксперт ИБ)
Поохотимся... на «черных лебедей»!
- 114** **Обратная связь / Павел РОГОВ**
(читатель BIS Journal)
Призрак русского хакера в Лондоне

ОФТОПИК

- 116** **Блогеры улыбаются**
Юмор



ОТЧЕТ GROUP-IB: ПОХИЩЕНО 3,8 МЛРД РУБЛЕЙ

Group-IB — одна из международных компаний, специализирующихся на предотвращении киберпреступлений — представила ежегодный отчет об исследовании рынка высокотехнологичных преступлений.

За последний год в России киберпреступники похитили 3,8 млрд рублей. 2,5 млрд рублей из них украли всего пять преступных групп, атаковавших банки. Их успех приведет к дальнейшей переориентации наиболее опытных преступников с компаний на банки, считают эксперты.

У компаний, в свою очередь, удалось похитить чуть меньше 1 млрд рублей. Характерно, что все новые вредоносные программы для хищений у компаний позволяют манипулировать отображением данных в браузере и делать хищения незаметными.

Зафиксирован и взрывной рост числа успешных атак на пользователей Android-

устройств, потерявших от действий хакеров 348,6 млн рублей — на 471% больше, чем в прошлом периоде. Мобильные тро-яны для хищений у физических лиц практически полностью вытеснили вирусы для ПК. Последними теперь занимается только одна преступная группа, а ущерб от ее действий составил 6,5 млн рублей.

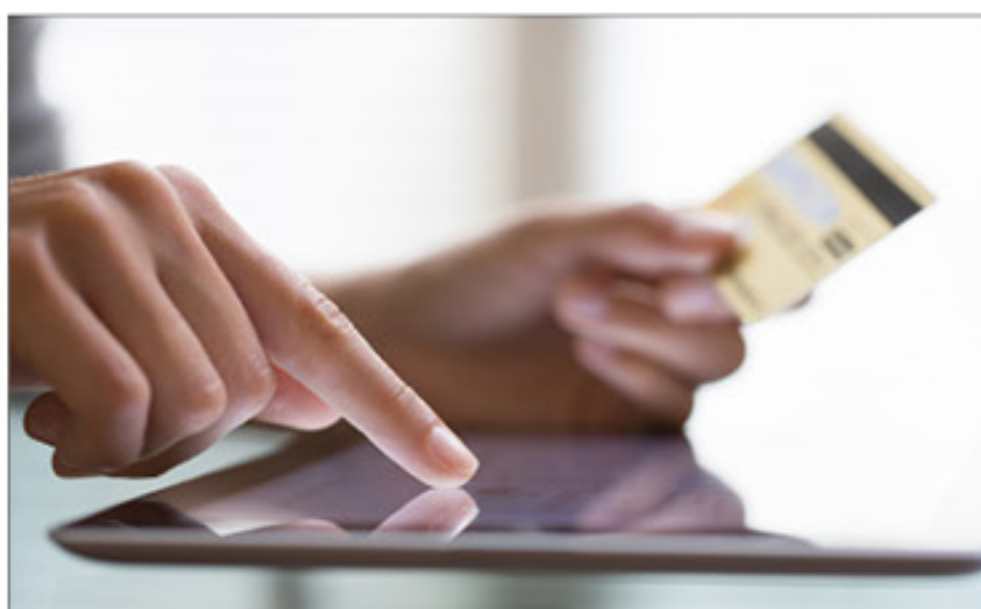
Внимание хакеров привлекает и индустрия «интернета вещей»: IoT-устройства, не защищенные антивирусами, стали главным драйвером роста бот-сетей для DDoS-атак.



ПОЛЬЗОВАТЕЛИ УСТАЛИ ОТ ПРОБЛЕМ БЕЗОПАСНОСТИ

Национальный институт стандартов и технологий США опубликовал результаты исследования отношения пользователей к вопросам кибербезопасности.

Постоянные разговоры в СМИ и социальных сетях о киберугрозах и необходимости борьбы с ними привели к ровно противоположному результату. Исследователи выделяют «усталость от проблем безопасности» как доминирующее настроение среди пользователей.



«Защититься от хакеров невозможно, это слишком сложно для моих мозгов, они даже АНБ взламывают, что уж о нас говорить», — таковы типичные высказывания. Эта позиция усиливается уверенностью в том, что ими — обывателями — хакеры наверняка не заинтересуются. «Я отправила подруге рецепт моих черничных кексов — ну, если хакеры перехватят сообщение, пусть пользуются...»

Чтобы переломить эту тенденцию, разработчики ПО должны максимально облегчить для пользователей задачу обеспечения кибербезопасности. С другой стороны, сами пользователи должны понять, что абсолютно любая информация, попав в руки хакеров, может вести к ущербу и содействовать новым преступлениям. Такое понимание продемонстрировали некоторые участники исследования. А именно те, кто уже стал жертвами кибератак.

ПЕРВЫЙ В РОССИИ ПРОМЫШЛЕННЫЙ CERT



«Лаборатория Касперского» открывает первый в России центр реагирования на компьютерные инциденты на индустриальных и критически важных объектах — Kaspersky Lab ICS-CERT.

Основная цель ICS-CERT — координировать действия производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей в области информационной безопасности. CERT будет собирать информацию об уязвимостях, инцидентах и актуальных угрозах и на основе этих данных предоставлять рекомендации по защите индустриальных и критически важных инфраструктурных объектов. Все данные, за исключением конфиденциальных, будут доступны публично в обезличенном виде.

SWIFT СТИМУЛИРУЕТ БАНКИ



Система SWIFT объявила о введении собственного стандарта безопасности. Объявленные требования включают 16 мер контроля и станут обязательными к исполнению для всех клиентов.

Вступление требований в силу произойдет в марте 2017 года. SWIFT оставляет за собой право запросить дополнительное подтверждение степени выполнения требований в виде результатов внутреннего или внешнего аудита. В случае невыполнения требований информация будет доводиться до регуляторов клиента.

К такому шагу руководство SWIFT подтолкнуло быстро растущее количество инцидентов, сигнализирующее о том, что клиентами не реализованы элементарные меры по безопасности, рекомендованные SWIFT и требуемые локальными регуляторами, в частности, Центробанком РФ.

**СБЕРБАНК И MICROSOFT
ОБЪЯВИЛИ О СОТРУДНИЧЕСТВЕ**

На Финополисе-2016 в Казани Сбербанк и Microsoft в России заключили договор о стратегическом сотрудничестве в области кибербезопасности.

«Для нас критически важно создать современный центр противодействия киберпреступникам, способный защитить российский бизнес, — заявил заместитель председателя правления Сбербанка Станислав Кузнецов. — А Microsoft обладает уникальной методологией выявления угроз и противодействия им в режиме реального времени. Использование экспертизы и технологических решений корпорации помогут нам сформировать свою экосистему в этой области».

После создания центра Сбербанк планирует оказывать услуги в сфере киберстрахования, консалтинга и обучения.

МИНКОМСВЯЗИ РФ: SMS ПРЕДСТАВЛЯЕТ УГРОЗУ ДЛЯ БАНКОВ

По мнению экспертов Минкомсвязи РФ, аутентификация пользователей по SMS представляет угрозу для банков.

Эксперты поясняют: уязвимость представляет не сама технология формирования кода, а SMS-канал, по которому он доставляется от банка пользователю. Существует несколько способов компрометации такого канала, например, злоумышленники могут заразить устройство пользователя трояном, способным перехватывать SMS с кодами, или перевыпустить SIM-карту с номером жертвы, воспользовавшись поддельным удостоверением личности. Таким образом со счетов россиян ежегодно похищается более 50 млн руб. И эта цифра в последнее время стремительно растет.

В качестве альтернативы предлагается применять генераторы одноразовых паролей (TOTP) с дополнительной защитой

при помощи шифрования. Для создания одноразовых паролей можно использовать сервисы «Яндекс. Ключ» или Google Authenticator. Пользователю нужно установить на свой планшет или смартфон соответствующую программу. Она подключается к сайту и генерирует одноразовые пароли с ограниченным сроком действия. При авторизации пользователю нужно будет вводить не старый, а новый одноразовый пароль.



ЛИЦЕНЗИИ ФСБ И ФСТЭК

www.vinser.ru
Тел.: +7 (495) 640-29-68
E-mail: vinsen@centro.ru

Вот уже более 10 лет наша компания предоставляет услуги по лицензированию. Команда специалистов с огромным опытом работы решит все Ваши проблемы по получению лицензии ФСТЭК и ФСБ, аттестации рабочих мест (АРМ) и помещений, обучению сотрудников, сертификации Вашей системы менеджмента качества (СМК).

- Консультирование по получению лицензий
- Подготовка полного пакета документов
- Аттестация рабочих мест и помещений
- Обследование информационной безопасности
- Обучение сотрудников
- Поиск и найм опытных специалистов
- Сертификация вашей СМК

Клиенты:



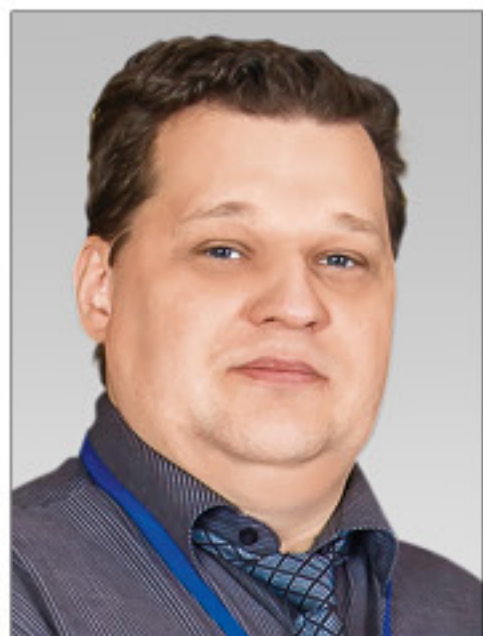
При заказе лицензии ФСБ или ФСТЭК Вы получаете планшет Samsung Galaxy Tab 4 7.0 в подарок!
Введите подарочный код «BISJ-10-reqw» на нашем сайте vinsen.ru при оформлении заказа.

SOC-FORUM

V.2.0

16.11.2016

SOC-FORUM.IB-BANK.RU



Александр ВИНОГРАДОВ
начальник Управления ИБ
АО КБ «Златкомбанк»



Фарит МУЗИПОВ
CISA, CISM, CRISC,
руководитель отдела ИБ
ООО КБ «АйМаниБанк»



Владимир ГОЛОВАНОВ
заместитель научного
директора
ООО НПФ «Кристалл»

СТО БР ИББС. ПО СЛУЧАЮ ЮБИЛЕЯ

Сколько лет комплексу стандартов Банка России?

В этом году сообщество банковских безопасников отмечает свой маленький юбилей. Ровно 10 лет назад была введена в действие вторая редакция Стандарта Банка России СТО БР ИББС-1.0–2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

Несмотря на то, что первая редакция Стандарта была принята в 2004 году, именно со второй редакции для многих безопасников начался процесс внедрения стандарта. Объясняется это прежде всего тем, что только в 2007 году было принято ещё два новых стандарта Банка России, формировавших основу для работ по оценке соответствия. Это СТО БР ИББС-1.1–2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» и СТО БР

ИББС-1.2–2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0–2006».

Трехлетний интервал между принятием стандарта требований (СТО БР ИББС-1.1–2004) и первых редакций стандартов оценки соответствия (СТО БР ИББС-1.1–2007 и СТО БР ИББС-1.2–2007) объяснялся периодом апробации стандартов оценки соответствия, как в кредитных организациях, так и в территориальных учреждениях Банка России. Например, в Центральном банке РФ в 2005 году была организована опытная зона, включавшая 10 территориальных учреждений Банка России (по существовавшему тогда административно-территориальному делению подразделений Банка

России), в которых должен был быть реализован весь комплекс мероприятий от реализации стандарта требований до работ по оценке (самооценке) соответствия.

Введение в действие Стандарта для Центрального Банка было знаковым событием. Регулятору пришлось переступить через многие свои правила. Во-первых, Центральный Банк впервые активно подключился к процессам, направленным на повышение защищенности участников отечественного финансового рынка — обеспечения как их информационной безопасности, так и их клиентов. Во-вторых, признал за банками право не следовать всем требованиям документа, а последовательно развивать свои системы обеспечения информационной безопасности через применение оценки зрелости процессов безопасности, которая была тем выше, чем полнее банк следовал требованиям Стандарта. В-третьих,



Стандарт был добровольным. Несмотря на это, Стандарт был положительно воспринят банковским сообществом. С каждым годом росло число банков, которые присоединялись к нему. И чтобы разобраться в причинах успеха, нужно вернуться к истокам.

В конце ноября 2003 года на базе научно-производственной фирмы «Кристалл» (г. Пенза) прошло первое заседание подкомитета «Защита информации в кредитно-финансовой сфере», входящего в состав 362-го технического комитета «Защита информации» Госстандарта России. Этот подкомитет был образован по инициативе Банка России в целях формирования экспертной площадки для выработки и обсуждения направлений развития процессов обеспечения и аудита информационной безопасности в кредитно-финансовых организациях России. Среди технических вопросов, вызвавших наиболее жаркие дискуссии на этом заседании

подкомитета, выделялась проблема разработки банковского стандарта по обеспечению информационной безопасности в кредитно-финансовой сфере и подходов к аудиту его реализации.

Основными источниками разработки стандарта явились следующие документы:

- ♦ международные и зарубежные стандарты и документы: ИСО/МЭК 17799, ИСО/МЭК 13335, ИСО/МЭК 21827, COBIT, OSTATE, BS 7799-2;
- ♦ национальные стандарты: ГОСТ 1.1-2002, ГОСТ Р 51898, ГОСТ Р 51897, ГОСТ Р ИСО/МЭК 15408;
- ♦ нормативные акты Банка России: 130-П, ВТ-60, 21-П, 3-П, 70-Т;
- ♦ другие документы.

В деятельности подкомитета приняли активное участие (вошли в состав ТК 362 и банковского подкомитета) такие организации, как банки «Петрокоммерц» и «Российский кредит», Институт Банковского Дела АРБ, между-

народная аудиторская фирма КПМГ и многие другие.

Была проведена очень большая кропотливая работа — и вот, наконец, долгожданная и важная новость: распоряжением Председателя Банка России С. М. Игнатъева (№ 609-Р от 18.11.2004) с 1 декабря 2004 года вводится в действие стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2004). Текст стандарта был опубликован в Вестнике Банка России от 24 ноября 2004 года № 68 (792).

Как уже отмечалось, стандарт прошел обкатку в нескольких крупных и небольших банках (Банк «Петрокоммерц» — в настоящее время входит в банковскую группу ФК «Открытие», «Метробанк») и, прежде всего, в самом Центральном Банке. Всю деятельность в рамках обеспечения ИБ



организации в соответствии с положениями СТО БР ИББС-1.0-2004 предлагалось «выстраивать» относительно «состояния защищенности интересов (целей) организации БС РФ в условиях угроз в информационной сфере» (определение понятия «информационная безопасность организации банковской системы Российской Федерации»). Защищенность интересов (целей) организации БС РФ безусловно лежит в плоскости основной деятельности — «основных процессов», тогда как деятельности и системы менеджмента ИБ составляют вспомогательные относительно основной деятельности, которые предназначены для обеспечения состояния защищенности интересов (целей) организации в информационной сфере. Позиционирование деятельности по обеспечению ИБ как вспомогательной деятельности обусловлено тем, что деятельности и системы менеджмента ИБ, включая соответствующие процессы, напрямую не участвуют в выпуске продукции организации, а наоборот добавляют себестоимости продукции и по своей сути являются затратными для организации. В то же время затраты на системы менеджмента ИБ создают экономию при возможных потерях (они их минимизируют), т.е. формируют прибыль, и по этой характеристике процессы системы менеджмента ИБ можно было бы отождествить с основными процессами.

Для формирования нормативной базы по ИБ Банка России в соответствии с требованиями Стандарта СТО

БР ИББС как результата деятельности и процессов по обеспечению ИБ требовался предварительный анализ формализованных процессов основной деятельности Банка России.

Необходимо было усовершенствование СТО. Было проведено не одно заседание 362 комитета и в конечном итоге: распоряжением Председателя Банка России С. М. Игнатъева (№ Р27 от 26.01.2006) с 1 января 2006 года вводится в действие стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2006). Это уже была вторая редакция Стандарта.

Но мало было принять Стандарт, нужно было убедить банки внедрять его. Центральный Банк провел большую работу по популяризации Стандарта. Заместитель начальник Главного управления безопасности и защиты информации Банка России Андрей Петрович Курило принял участие в ряде форумов и конференций, посвященных информационной безопасности, продвигая идею Стандарта. На уфимской

конференции «Банки. Процессы. Стандарты. Качество» стандарту СТО БР ИББС была посвящена целая секция. Со временем она переросла в самостоятельную международную конференцию Уральский форум «Информационная безопасность банков», который в 2017 году будет проводиться в девятый раз. С целью продвижения Стандарта было создано Сообщество пользователей стандартов Банка России по информационной безопасности (Сообщество ABISS), которое было призвано объединить всех участников процесса обеспечения информационной безопасности банков: Центральный Банк, коммерческие банки, интеграторов, учебные заведения. Активную поддержку Стандарту оказал Комитет по информационной безопасности АРБ. И усилия не пропали даром: Стандарт зашагал по стране.

Многие кредитно-финансовые организации начали присоединяться к СТО. Появились документы по обеспечению ИБ в банках. Специалисты уже начали выстраивать свою работу и осознавать, что информационная безопасность — это уже не пустой звук, а та цель, к которой нужно стремиться при выстраивании всей этой цепочки у себя.

Но работа, документы и др. — это все хорошо, но как оценить себя — насколько банк готов. Для этих целей в 2007 году был принят ряд документов, включая упоминавшиеся ранее, в частности, следующие:

- ♦ СТО БР ИББС-1.1-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информа-

Распоряжением Председателя Банка России С. М. Игнатъева (№ Р27 от 26.01.2006) с 1 января 2006 года вводится в действие стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2006)

ционной безопасности» (распоряжение Р-345 от 28 апреля 2007);

♦ СТО БР ИББС-1.22007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0–2006» (распоряжение Р-346 от 28 апреля 2007);

♦ РС БР ИББС-2.0–2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требова-

ниями СТО БР ИББС-1.0» (распоряжение Р-348 от 28 апреля 2007);

♦ РС БР ИББС-2.1–2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0» (распоряжение Р-347 от 28 апреля 2007).

Но в то же время Стандарт не был просто бумагой, содержащей требования по информационной безопасности. Он инициировал процесс формирования сообщества банковских

безопасников. Бороться с современными вызовами информационной безопасности можно только сообща, и сильная корпорация банковских безопасников является хорошим подспорьем. Сейчас у нас есть и FinCERT, и Клуб «Анти-фрод». Но не будем забывать, что когда-то это все началось со Стандарта и Сообщества «ABISS» как инструмента его продвижения. В настоящее время Стандарт переходит на новый уровень. На его основе подготовлен проект национального стандарта, предназначенный для применения в соответствии с действующим законодательством (№ 184-ФЗ от 2002 года «О техническом регулировании» и № 162-ФЗ от 2015 года «О стандартизации»).



Андрей КУРИЛО

доцент Финансового университета при Правительстве Российской Федерации, председатель Комитета по информационной безопасности НП НСФР, кандидат технических наук

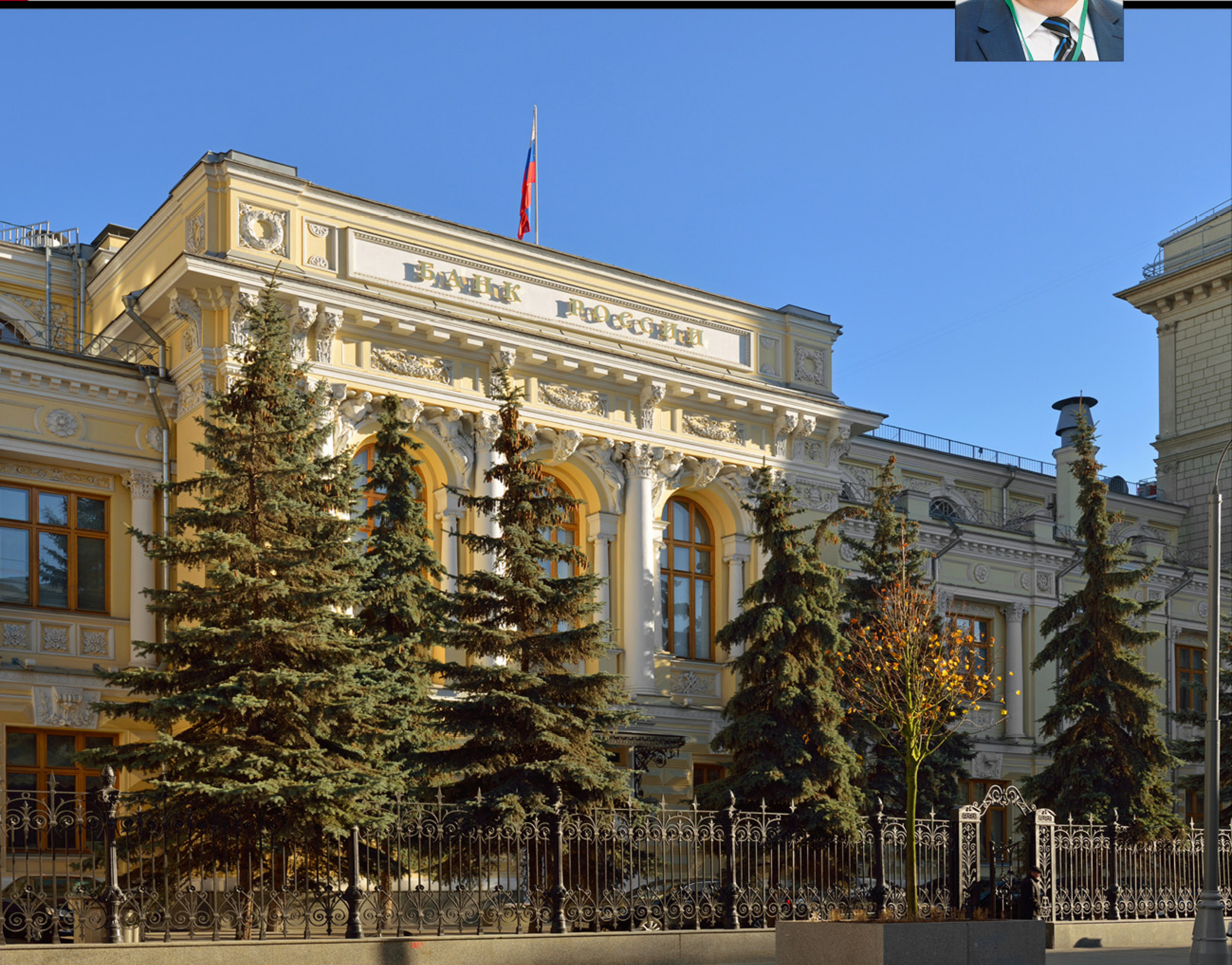
Идея создания для банковской системы единого набора требований по информационной безопасности и как следствие единого и универсального набора критериев оценки уровня информационной безопасности кредитной организации возникла еще в 2000 году.

Банк России провел работу по изучению данного вопроса в ряде ведущих зарубежных банках, были изучены все имеющиеся на то время зарубеж-

ные национальные и международные стандарты, стандарты аудита. Нам стало понятно, с учетом общего состояния вопроса в стране и в банковском сообществе, а также существующего нормативно — правового поля, опираться на зарубежные стандарты путем их прямого заимствования нецелесообразно и неправильно. В первую очередь это было связано с тем, что реализация в полном объеме требований имевшихся на то время международно признанных стандартов безопасности BSI 7799 и ISO 27001 была крайне затруднительна для кредитных организаций. Поэтому специалисты Банка России пришли к выводу о необходимости разработки, с учетом положений указанных стандартов, собственного комплекта документов, с включением в него идеологии стандартов качества ISO 9000 и стандарта аудита COBIT в части использования рейтингового подхода к оценке достигнутого уровня безопасности, известного как «шка-

ла зрелости». Как показала дальнейшая практика, такой подход оказался верным и позволил провести в банковской системе Российской Федерации радикальное улучшение положения дел. С удовлетворением следует сказать, что по уровню глубины проникновения стандартов в среду регулирования, комплекс стандартов Банка России СТО ИББС занимает одно из первых мест. Новый мощный толчок этой теме придал Федеральный закон «О Стандартизации в Российской Федерации», в соответствии с которым появилась возможность после перевода стандартов предприятия, которыми являются стандарты комплекса СТО ИББС, в статус государственных стандартов включать их требования в состав нормативных документов Банка России. Таким образом будет преодолено известное противоречие между рекомендательным статусом Стандарта и обязательностью требований безопасности, включенных в него.

BIS-КОММЕНТАРИЙ



КИБЕРБЕЗОПАСНОСТЬ ФИНРЫНКА

*Первый годовой отчет FinCERT Банка России.
Комментарии, заметки на полях*

В июне 2015 года Банк России объявил о начале работы Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT). В его задачи входят сбор информации о кибератаках и оперативное оповещение о киберугрозах участников финансового рынка, взаимодействующих в области обмена информацией с FinCERT. Результаты деятельности FinCERT с июня 2015 по май 2016 года обобщены в годовом отчете. Среди безусловных плюсов — фиксация более 20 крупных информационных атак на российские банки, блокировка десятков фишинговых доменов в зоне RU. Сводный анализ позволяет оценить результаты работы за год, а также определить задачи на будущее.

ИНФОРМАЦИОННЫЙ ОБМЕН ВЫСТРОЕН

Необходимость создания в Банке России подразделения для оперативного реагирования на компьютерные атаки в кредитно-финансовой сфере назрела к концу 2014 года. Ранее вопросы кибербезопасности финансовых ор-

ганизаций рассматривались на Совете Безопасности Российской Федерации. В июне 2015 года начал работу FinCERT — Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России.

За год, прошедший с начала работы FinCERT, был выстроен информационный обмен с ФСБ России, МВД России и Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА). К этому взаимодействию подключились около 300 кредитных организаций, платежные системы, операторы связи и разработчики программного обеспечения.

Сотрудники FinCERT организовали регулярное оповещение участников информационного обмена о выявленных уязвимостях и информационных угрозах. Начиная с 1 января 2016 года, была выполнена 141 рассылка, инициирована блокировка 341 домена, которые использовались злоумышленниками для сбора информации конфиденциального характера, распространения вредоносного программного обеспечения и спама.

Киберпреступники тоже не стоят на месте: постоянно совершенствуют свой инструментарий, быстро реагируют на нововведения. С начала работы FinCERT злоумышленники неоднократно пытались провести рассылку электронных документов с вредоносными кодами от имени Банка России и клуба «Антидроп».

С массовыми мошенническими рассылками FinCERT сталкивается практически ежедневно, отмечая, что их каналы и форматы постоянно меняются. Если прежде злоумышленники в основном использовали электронную почту и SMS-сообщения, то за последние полгода все чаще задействуют мобильные мессенджеры типа Viber, WhatsApp и т.п.

Специалисты FinCERT анализируют полученную информацию о рассылках: масштабы, содержание, разновидности вредоносного кода и другие параметры. Анализ полученной информации позволяет делать выводы о степени опасности для организаций кредитно-финансовой сферы и определять приоритетность обработки. Сотрудники FinCERT рассылают бюллетени с перечнем угроз и их параметрами — тек-

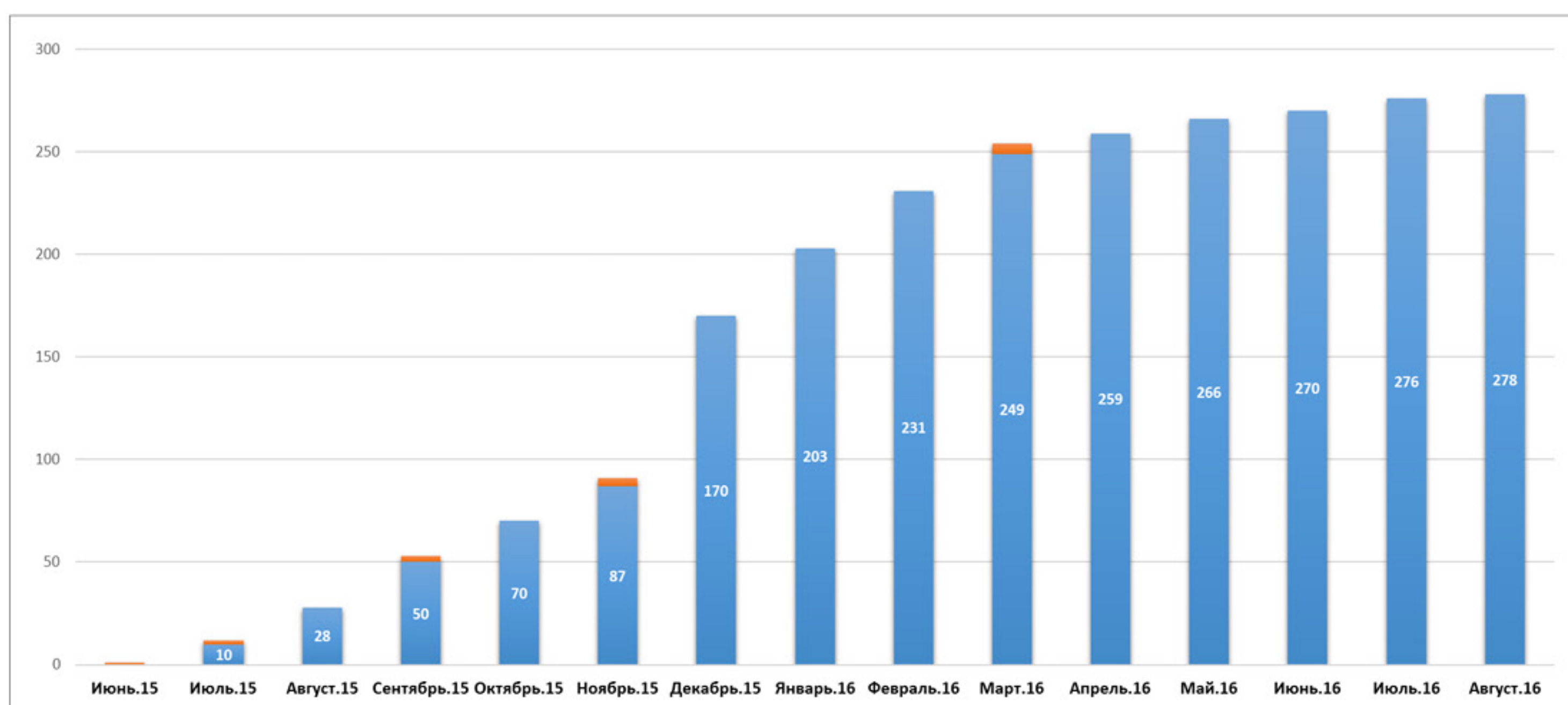


Рисунок 1. Динамика присоединения кредитных организаций к информационному обмену

стами сообщений с указанием операторов мобильной связи и номеров мобильных телефонов, с которых ведется атака, доменных имен и т.п., что позволяет участникам информационного обмена провести своевременную блокировку нежелательной информации. Этот отлаженный механизм взаимодействия позволяет в самые короткие сроки собирать, анализировать и доводить актуальную информацию до участников информационного обмена.

СКРЫВАТЬ ИНЦИДЕНТЫ — СЕБЕ ДОРОЖЕ

Одним из значимых событий в сфере кибербезопасности в первый год работы FinCERT можно считать задержание правоохранительными органами организованной преступной группы, которая занималась хакерскими атаками на платежную систему Банка России. В средствах массовой информации эту группу хакеров называли Lurk. Впервые в отечественной практике было заведено уголовное дело одновременно по двум статьям Уголовного кодекса Российской Федерации — «Организация преступного сообщества или участие в нем» и «Мошенничество в сфере компьютерной информации», задержаны около 50 участников преступной группы.

Атаки этой хакерской группы на корреспондентские счета кредитных организаций стали предметом внимания FinCERT с самого начала его работы. Первые атаки на процессинговые центры были зафиксированы еще в конце 2015 года. По предварительным данным на конец июля, группировка пыталась похитить порядка 2,5 млрд рублей,



Рисунок 2. Процесс обработки информации в FinCERT

но благодаря налаженному взаимодействию Банка России с правоохранительными органами и кредитными организациями, вывод части средств был приостановлен. Вместе с тем сумма, которую злоумышленникам все-таки удалось вывести, составила около 1,6 млрд рублей.

Анализ наработанного за год опыта выявил проблемы, которые предстоит решать. Прежде всего, это недостаточное понимание менеджментом кредитных организаций важности требований информационной безопасности. Работа FinCERT показала: руководство многих банков недостаточно четко понимает роль информационной безопасности в современном мире, важности обмена данными о компьютерных инцидентах. Подключиться к работе FinCERT, пользоваться его наработками, сводками и материалами — необходимо, но этого мало. Важно сообщать сведения об инцидентах нарушения информационной безопасности в своей организации.

Основной недостаток менеджмента ряда банков — упрощенный взгляд на взаимодействие с FinCERT. Некоторые участники информационного обмена работают в режиме получения информации, пренебрегая обратной связью. Такая линия не является конструктивной, поскольку сведения об инцидентах в области информационной безопасности в одной организации представляют интерес для остальных. Они могут ока-

заться решающими для выявления новых угроз, противодействия хакерским атакам. Поэтому обмен такой информацией должен быть взаимным, тем более, что он является анонимным: информация об организации, которая подверглась атаке, не раскрывается.

Необходимо понимание со стороны менеджмента банков важности передачи регулятору данных об инцидентах в сфере информационной безопасности. Со стороны Банка России будет усилено нормативное регулирование отрасли: предстоит подготовка и выпуск нормативных документов как рекомендательных, так и обязательных для исполнения.

КОМУ ПРЕДСТОИТ РАБОТА НАД ОШИБКАМИ

Еще одна достаточно типичная проблема, которая была выявлена за год работы FinCERT, — это финансирование обеспечения информационной безопасности по остаточному принципу, которым грешат некоторые банки. Крупные банки, как правило, уделяют должное внимание информационной безопасности и финансированию ее обеспечения. Некоторые средние и мелкие банки выделяют на эти цели недостаточно средств. Поэтому нам предстоит разработать механизм, обязывающий менеджмент находить необходимые средства и выделять их.

Такую необходимость диктует жизнь: мошеннические схемы развиваются и совершенствуются. Первые атаки осуществлялись на физических лиц и отдельные организации, потом начались массовые DDoS-атаки и атаки на банки. С появлением таргетированных атак в 2011–2012 годах участились случаи нападения хакеров на платежную систему Банка России и международную систему SWIFT.

Подключиться к работе FinCERT, пользоваться его наработками, сводками и материалами — необходимо, но этого мало. Важно сообщать сведения об инцидентах нарушения информационной безопасности в своей организации

Ещё одна достаточно типичная проблема, которая была выявлена за год работы FinCert, — это финансирование обеспечения информационной безопасности по остаточному принципу, которым грешат некоторые банки

Уязвимы не только банковские автоматизированные системы, но и другие информационные финансовые сервисы. Хакеры могут активно действовать в секторе небанковских финансовых организаций — на биржах, атаковать брокерские компании и т.д. Злоумышленники могут проявить активность во многих новых направлениях, поэтому предстоит расширение работы совместно с правоохранительными органами, со стороны которых мы видим полное взаимопонимание.

Поводы для оптимизма есть. Не так давно информационная безопасность в некоторых кредитно-финансовых организациях строилась по инерции, по принципам безопасности традиционного бумажного документооборота. Но сейчас как топ-менеджмент, так и руководители, и специалисты профильных подразделений начинают понимать специфику информационной безопасности и важность серьезного отношения к ней.

Поднадзорные Банку России организации все чаще обращают внимание на необходимость использования современных технических средств защиты информации, все более целенаправленно выстраивают эшелонированные системы защиты. Крупные банки создают собственные центры оперативного управления информационной безопасностью — SOC для противодействия атакам типа APT (advanced persistent threat) — целевой развитой устойчивой угрозы. Банки также тестируют и внедряют в свою деятельность системы фрод-мониторинга.

Для увеличения скорости взаимодействия прорабатывается возможность

перехода к новым форматам информационных бюллетеней FinCERT. Объемы направляемой FinCERT информации неуклонно растут, и участники информационного обмена предлагают перейти на автоматизированную обработку бюллетеней в машиночитаемых форматах OpenIOC, Yara, STIX, XML и т.п.

НАЗРЕВШИЕ ИЗМЕНЕНИЯ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ

Повышение эффективности противодействия киберпреступности в кредитно-финансовой сфере требует развития нормативно-правовой базы, в том числе на уровне федерального законодательства. 3 июня 2016 года прошло совещание Правительства Российской Федерации, посвященное вопросам информационной безопасности в кредитно-финансовой сфере, на котором рассматривались в том числе вопросы внесения изменений в законодательство.

Так, Сбербанк России разработал поправки в Уголовный кодекс Российской Федерации, руководство банка и депутат Госдумы Российской Федерации Илья Костунов подготовили законопроект об изменении статей, касающихся компьютерных преступлений. Банк России поддержал данную законодательную инициативу.

Проблема компьютерных преступлений, включая мошенничества с помощью высокотехнологичных инструментов, особенно остро стоит в банковской сфере. Правоприменительная практика рассматривает данные преступления согласно главе 28 Уголовного кодекса Российской Федерации и подпунктам о мошенничестве. Ранее, в 2011 году, в главу 28 УК РФ (ст. 272, 273 и 274) были внесены изменения, которые ужесточали наказания за такие преступления. Но на практике выявился ряд сложностей, связанных как с квалификацией неправомерного доступа к компьютерной информации, так и с процессуальным оформлением доказательств.

Принятие поправок, разработанных с участием Сбербанка России, позволит сделать серьезные шаги в борьбе с высокотехнологичным криминалитетом в кредитно-финансовой сфере. Это подтверждается и зарубежным опытом, особенно США и Великобритании, где в уголовном законодательстве

FinCERT выявил основные недостатки в области информационной безопасности у организаций кредитно-финансовой сферы, которые привели к удачным кибератакам:

- ♦ наличие уязвимостей в системах безопасности автоматизированных информационных систем организаций и платежных приложений;
- ♦ недостатки обеспечения информационной безопасности, отсутствие должного соблюдения ими требований, установленных нормативными актами и отраслевыми стандартами Банка России;
- ♦ отсутствие должного внимания менеджмента к использованию безопасных технологий, в том числе для осуществления переводов денежных средств;
- ♦ отсутствие должной координации деятельности по противодействию массовым (веерным) и типовым компьютерным атакам.

компьютерные преступления тщательно детализированы. Различные противоправные действия — кража паролей, DDoS-атаки и т.д. — квалифицируются каждое по отдельности. У нас пока действует определение этих разнообразных видов преступлений как неправомерного доступа к информации, за что предусматривается уголовная ответственность, несоизмеримая с серьезностью и опасностью данных правонарушений.

В ближайшее время должен быть восполнен еще один пробел в нормативно-правовой базе, мешающий выстраивать безопасное информационное пространство в кредитно-финансовой сфере. Необходимо разработать и официально принять критерии определения неправомерных платежей. Требуется ввести классификацию признаков подозрительного платежа, что позволит своевременно приостанавливать такие транзакции до результатов разбирательства. Это сильно осложнит жизнь злоумышленникам. Кроме того, необходимо узаконить обмен информацией между банками и правоохранительными органами о дропперах — лицах, занимающихся выводом и обналичиванием похищенных денежных средств. Для этого в нормативно-правовой базе должны появиться изменения, затрагивающие ряд положений федеральных законов о персональных данных и о банковской тайне. Необходимость таких изменений диктуется сложившейся практикой хищений и последующего вывода финансовых средств.

По инициативе Минфина РФ, при участии FinCERT Банка России, НП «Национальный совет финансовых рынков» подготовлен проект соответствующего нормативного акта. Четкая, детальная классификация компьютерных преступлений в кредитно-финансовой сфере позволит узаконить быстрый обмен информацией о попытках хищений и вывода средств, а также приостановить подозрительные транзакции. Надеемся, что вновь избранный состав Государственной Думы России достаточ-



Следует ожидать усиления нормативного регулирования информационной безопасности организаций кредитно-финансовой сферы на различных уровнях: федерального законодательства, ведомственных документов и национальных стандартов

но оперативно внесет вышеперечисленные изменения в федеральное законодательство, что создаст дополнительные возможности для банковского сообщества и правоохранительных органов по противодействию киберпреступности.

Следует ожидать усиления нормативного регулирования информационной безопасности организаций кредитно-финансовой сферы на различных уровнях: федерального законодательства, ведомственных документов и национальных стандартов. Некоторые рекомендательные нормы могут стать обязательными. Ответственность организаций кредитно-финансовой сферы за обеспечение информационной безопасности на местах будет усиливаться.

ВЗАИМОДЕЙСТВИЕ С ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ

За прошедший год FinCERT Банка России наладил и активно развивал сотрудничество с правоохранительными органами. В первую очередь это касается обмена информацией. Наибольший взаимный интерес представляет обмен аналитической информацией, тенденциями развития киберпреступлений, схемами

мошенничества, сведениями о подготовке киберпреступлений в кредитно-финансовой сфере. В результате появилась возможность во взаимодействии с правоохранительными органами оказывать эффективную помощь службам информационной безопасности банков.

После внесения изменений в законодательство Российской Федерации, о которых было сказано выше, будет налажен официальный обмен информацией о подозрительных транзакциях и дропперах. В этом обмене будут участвовать FinCERT Банка России, организации кредитно-финансовой сферы и правоохранительные органы.

За прошедший год работы FinCERT Банка России произошли кардинальные положительные сдвиги: все стороны информационного взаимодействия понимают необходимость и проявляют заинтересованность в совместной работе. Так, повысилась результативность противодействия криминалу, расследований инцидентов, увеличилось количество возбуждаемых уголовных дел.

Среди перспективных направлений взаимодействия с правоохранительными органами — создание FinCERT Банка России профильной лаборато-

рии экспресс-анализа. Деятельность лаборатории поможет организациям, поднадзорным Банку России, и правоохранительным органам в подготовке и проведении предварительных технических исследований носителей информации, полученных в результате оперативной проверки или оперативно-розыскных мероприятий.

Кроме того, на базе FinCERT Банка России планируется создание центра компетенций и анализа безопасности банковских технологий, информационных систем и программного обеспечения. Деятельность центра будет направлена на исследование новых перспективных технологий, способных затрагивать кредитно-финансовую сферу, прогнозировать риски и проблемы, с которыми можно столкнуться при их массовом внедрении. Обмен подобной информацией с правоохранительными органами позволит предотвращать новые разновидности киберпреступлений.

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

В функции FinCERT входит сотрудничество с международными правоохранительными органами — Интерполом, Европоллом, представителями зарубежных организаций участников TF-CSIRT — Компьютерной группы реагирования на чрезвычайные ситуации и т.п. Представители FinCERT посетили Малайзию и Францию, руководство провело переговоры о взаимодействии с крупными транснациональными корпорациями, специализирующимися на кибербезопасности и защите платежных систем.

Цели совместной работы на международной арене — оперативный обмен информацией. Информационный обмен коснется тенденций развития киберпреступности, готовящихся и уже совершенных киберпреступлений, и, что особенно важно, преступлений, организованных за рубежом. Важным результатом должно стать получение из-за рубежа оперативной информа-

FinCERT Банка России готов уделять повышенное внимание взаимодействию с международными организациями

ции о киберпреступлениях и соответствующих доказательствах.

FinCERT Банка России готов уделять повышенное внимание взаимодействию с международными организациями. Одной из задач Центра компетенций и анализа безопасности банковских технологий, информационных систем и программного обеспечения является развитие взаимодействия с центральными банками ближайших партнеров России, стран-участников Таможенного союза, ЕАЭС. На осень 2016 года намечены встречи представителей FinCERT Банка России с коллегами из Белоруссии и Казахстана.

Заинтересованность в обмене информацией проявляют все стороны. Наша общая цель — наладить оперативное взаимодействие, чтобы успешно противодействовать трансграничной киберпреступности. Сейчас, к сожалению, когда похищенные данные или денежные средства «пересекают» границу и подпадают под юрисдикцию другого государства, дальнейшее получение информации о них и возвращение похищенного становится практически невозможным.

Открытость государственных границ для деятельности киберпреступников мешает своевременно выявлять и предупреждать киберпреступления, расследовать и доводить до суда уже совершенные. Решать эту проблему можно только при активном взаимодействии правоохранительных органов разных стран, которое и предстоит выстроить.

ПЕРСПЕКТИВЫ АВТОМАТИЗАЦИИ

На июньском совещании, проведенном Правительством РФ, были учтены предложения Банка России, поддержанные финансовым и банковским сообществом. Реализация проекта повы-

шения информационной безопасности кредитно-финансовой сферы возложена на Главное управление безопасности и защиты информации Банка России, а решение ряда ключевых вопросов поручено FinCERT. Руководство Банка России уделяет огромное внимание проблеме информационной безопасности и оказывает всю необходимую помощь в развитии Центра. Увеличение количества и объемов обязанностей сопровождается расширением структуры: за прошедший год штат был увеличен в два раза, появились новые направления деятельности.

Одно из важнейших направлений — подготовка перехода с ручного режима на автоматизированную работу, то есть внедрение промышленного антифрода на базе системы платежей и электронных расчетов Банка России. Обмен информацией будет производиться оперативно, в автоматизированном безопасном режиме, что позволит намного быстрее реагировать на новые угрозы и инциденты. В перспективе возможно и создание лаборатории для проведения первичного анализа новых угроз и выявляемых уязвимостей в автоматизированном режиме. Возможно и создание информационной базы дропперов, работающей также в автоматическом режиме.

* * *

Перечисленные нововведения позволят вывести обмен данными между Банком России, организациями кредитно-финансовой сферы и правоохранительными органами на новый уровень, улучшит их взаимодействие и координацию работы. Рассмотренные в данной статье вопросы отражены в дорожной карте, которая размещена на официальном сайте Банка России.



Артём СЫЧЕВ
заместитель начальника
ГУБЗИ Банка России



Сергей ВИХОРЕВ
директор по ИБ филиала
«ПЕТЕР-СЕРВИС
Спецтехнологии»

ПОГОВОРИМ ОБ АУТСОРСИНГЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

*Эссе на тему, как Вовка
в Тридевятом царстве
аутсорсинг пользовал*

Тема аутсорсинга информационной безопасности в широком смысле этого термина (передача организацией, на основании договора, определённых видов или функций производственной предпринимательской деятельности другой компании, действующей в нужной области) сейчас на слуху, тема горячая, разве что ленивый не писал на эту тему. Авторы не ленивы, за темой следят, а сподвигло авторов взяться за клавиатуру упоминание 06.07.2016 г. в Твиттере А. Прозоровым о разработке одной из компаний (не называем ее, здесь нет места рекламе!) проекта рекомендаций Банка России «Аутсорсинг информационной безопасности», который благополучно размещен на сайте ТК 122.



На взгляд авторов, этот проект представляет собой гибрид между рекламным буклетом системы мониторинга и популяризирующей это направление журнальной статьей, и в этом документе не хватает только одной фразы: «Покупайте наших слонов! Наши слоны — самые слонистые слоны в России! Россия — родина слонов!» Авторам кажется, что подходить к проблеме аутсорсинга так узко — просто неприлично. Это же широчайшее поле деятельности! Вот и родилась идея продолжить наши диалоги, немного обобщить уже существующий опыт аутсорсинга безопасности информации (все-таки так правильнее, чем «информационной безопасности»), добавить свое видение проблемы и попытаться положить эти мысли на бумагу и расставить все точки над «i». А поможет в этом Вовка из Тридевятого царства, который, наверное, один из первых применил схему аутсорсинга, хотя и не всегда удачно. Что получилось — судить, как всегда, Вам, читатель.

ВМЕСТО ПРОЛОГА. ЧТО ЖЕ ЭТО ЗА ЗВЕРЬ ТАКОЙ — АУТСОРСИНГ?

Итак, начнем от печки. Аутсорсинг (от англ. *outer-source-using* — использование внешнего источника и/или ресурса) — передача организацией, на основании договора, определенных видов или функций производственной предпринимательской деятельности другой компании, действующей в нужной области. И уж, конечно, это не «форма организации труда», как указано в проекте, это договорные обязательства: одна сторона поручает что-то сделать, а другая это поручение исполняет, а уж как она «организует труд» — не важно, важен процесс и результат. Правовая основа его сложна. Здесь есть элементы и аренды, и подряда, и услуги, и агентства, и поручительства. В общем, весь Гражданский кодекс. Хотя больше всего здесь именно услуги: ведь заказчик услуги не всегда ставит во главу угла конечный резуль-

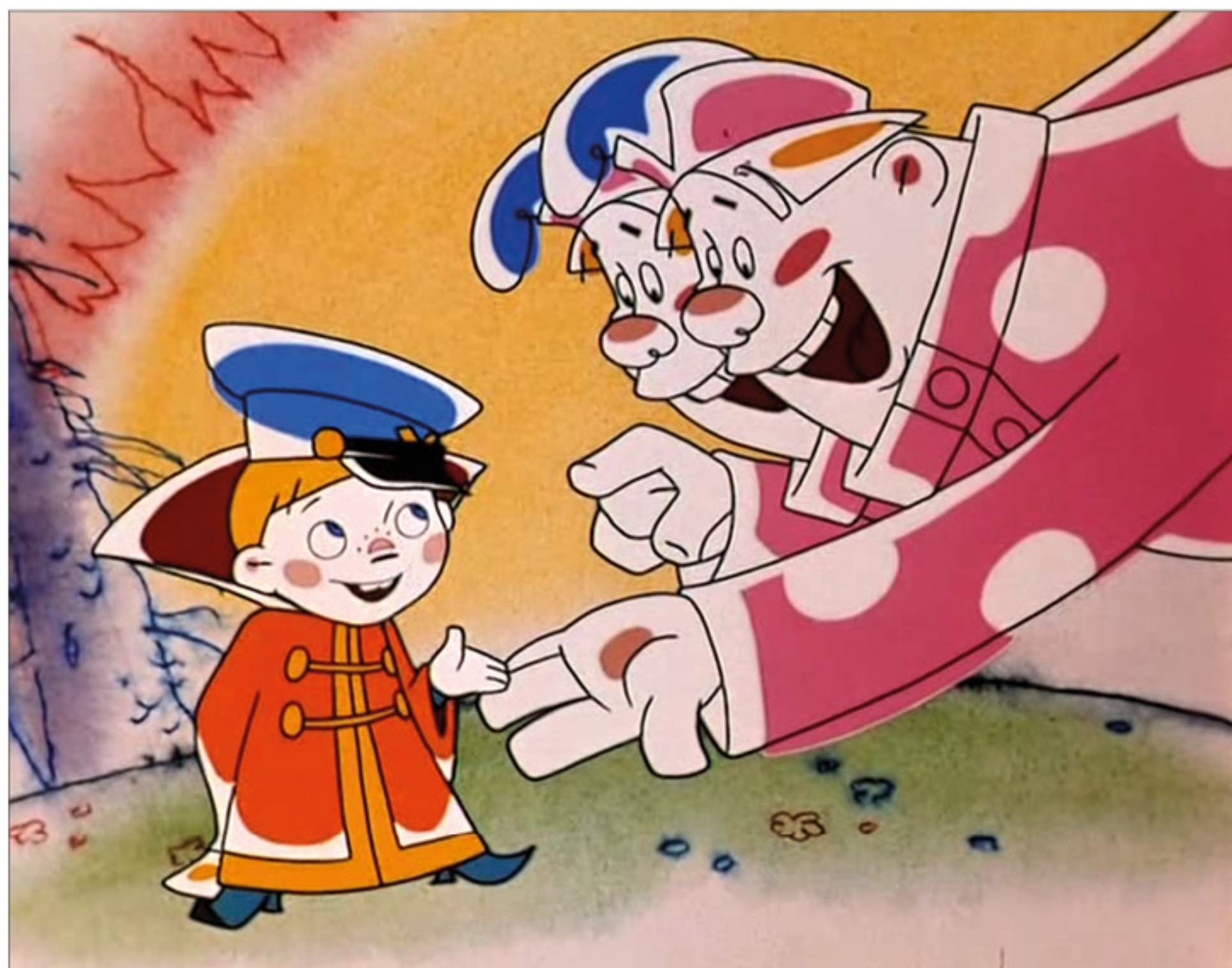
Передача функций обеспечения безопасности информации на аутсорсинг, конечно же, увеличивает риски безопасности информации. Поэтому, прежде чем принять такое решение, необходимо все взвесить и обосновать

тат, его больше интересует процесс, который будет исполнять поставщик. Правда, есть у аутсорсинга и отличительные черты: первая — он, как правило, предполагает долгосрочное сотрудничество поставщика (провайдера сервиса) и заказчика, хотя, возможны варианты. Вторая — при аутсорсинге, как правило, передаются целые процессы (производственные, бизнес-процессы) или отдельные функции. То есть при аутсорсинге всегда есть конечный бизнес-результат, который может быть сепарирован в компании-заказчика. Третья — это то, что поставщик услуг и заказчик «сливаются в экстазе». Не всегда можно точно сказать: то ли по-

ставщик интегрируется в структуру заказчика, то ли наоборот. В общем, они как сиамские близнецы: разорвать их уже нельзя. Вот и получается, что аутсорсинг — это содружество, можно сказать, партнерство, между поставщиком услуг и заказчиком, основанное на взаимном доверии, но подкрепленным целым ворохом юридических документов.

ЧАСТЬ 1. ЧТО ЖДАТЬ ОТ АУТСОРСЕРА

Передача функций обеспечения безопасности информации на аутсорсинг, конечно же, увеличивает риски безопасности информации. Поэтому



— Это вы и пальцы за меня загибать будете?

му, прежде чем принять такое решение, необходимо все взвесить и обосновать. В принципе, на аутсорсинг можно многое передать, но надо четко определиться с тем, какие функции передаются на аутсорсинг и есть ли в этом необходимость. А то можно так «напередать», что весь бизнес про...фукать. И главное, надо идти с открытым забралом, решение о передаче чего-либо на аутсорсинг должно быть осознано руководством заказчика и задокументировано надлежащим образом.

На аутсорсинг могут передаваться все наиболее ресурсоемкие функции обеспечения безопасности информации, связанные с подготовкой к принятию решения по обеспечению безопасности информации, подготовкой решения по принятию рисков безопасности информации, выполнению отдельных функций безопасности информации, проведению эксплуатации, обслуживанию и поддержанию в работоспособном состоянии средств защиты информации, оценке соответствия установленным требованиям.

Но! На аутсорсинг не могут и не должны передаваться функции, связанные непосредственно с принятием решений по обеспечению безопасности информации и (или) выбору требуемого уровня защищенности, а также функции, связанные с принятием рисков безопасности информации. От этого зависит судьба заказчика и поэтому выпускать решение этих проблем из своих рук — нельзя, это остается прерогативой заказчика. Ответственность за обеспечение безопасности информации при передаче даже большей части функций безопасности информации поставщику услуг, не может быть



— Это вы и конфеты за меня есть будете? Ну уж нет!

передана и всегда остается за заказчиком услуг. А поставщик услуг, в свою очередь, обязан будет выполнять требования документов заказчика, определяющих политику обеспечения безопасности информации.

Ну, и конечно же, решая, что передавать на аутсорсинг, надо помнить о том, что законодательство содержит прямой запрет на передачу сведений, составляющих банковскую тайну (ст. 857 ГК РФ) и налоговую тайну (ст. 102 НК РФ) третьим лицам, и поэтому процессы обработки информации, связанные с предоставлением поставщику услуг возможности ознакомления со сведениями, отнесенными к банковской тайне и налоговой тайне, не могут быть переданы на аутсорсинг.

Отношения между поставщиком и заказчиком услуг строятся на договорной основе. Здесь важно правильно оценить возможности поставщика. Далее мы отдельно поговорим об этом, а сейчас отметим, что поставщик услуг должен иметь необходимые силы и средства для оказания услуги. Плох тот поставщик, который не может оказать услугу самостоятельно и приглашает для этого своих контрагентов. Заключение договора с поставщиками услуг, допускающими привлечение третьих лиц (контрагентов) для оказания услуги, в рамках договора не целесообразно. Поставщик услуг должен иметь необходимые лицензии на выполнение работ и оказание услуг, предусмотренных законодательством Российской Федерации, квалифицированный персонал, процессы, методологии, технологии, необходимые для оказания услуги, и надежную репутацию. При заключении договора на оказание услуг очень важно определить конечный результат оказания такой услу-

Надо четко определиться с тем, какие функции передаются на аутсорсинг и есть ли в этом необходимость. А то можно так «напередать», что весь бизнес про...фукать

ги и критерии, позволяющие оценить результативность и качество исполнения услуги. Заказчик услуги должен вести надлежащий контроль за качеством исполнения услуги и ее результативностью. Поставщик услуг обязан предоставить заказчику услуг возможность и необходимые инструменты для осуществления такого контроля, в том числе и с привлечением независимых экспертов.

ЧАСТЬ 2. ЧТО МОЖЕТ АУТСОРСЕР

Как уже отмечали авторы, поставщик услуг может многое. Конечно, конкретные характеристики услуг (сервисов) безопасности информации зависят от возможностей и ресурсов поставщика услуг и определяются наличием у него квалифицированного персонала, отлаженных процессов и методологии, а также технологий защиты информации.

Чтобы иметь представление о том, что же он может на самом деле, надо все возможные услуги (сервисы) проклассифицировать и разложить по полочкам. Попробуем это сделать.

На основе анализа существующих на рынке услуг, предоставляемых различными поставщиками услуг (провайдером) все услуги (сервисы) безопасности информации можно разделить на несколько основных групп:

1. Управленческие сервисы безопасности информации.

- а. Услуга по организации (налаживанию) процесса обеспечения БИ
- б. Услуга по разработке (пересмотру) документов, определяющих политику БИ
- с. Услуга по управлению рисками БИ в организации
- д. Услуга по разработке архитектуры БИ в организации

2. Операционные сервисы безопасности информации

- а. Услуга повышения осведомленности (обучения) персонала организации
- б. Услуга управления безопасностью информации

Чтобы иметь представление о том, что же аутсорсер может на самом деле, надо все возможные услуги (сервисы) проклассифицировать и разложить по полочкам

- с. Услуга расследования инцидентов безопасности информации (форензика)
- д. Услуга технического обслуживания средств защиты информации
- 3. Технологические сервисы безопасности информации
 - а. Услуга по реализации мер защиты
 - б. Услуга по предоставлению защищенной инфраструктуры ИС
 - с. Услуги по оценке безопасности продуктов и ИС
 - д. Услуги по безопасной разработке прикладного программного обеспечения

е. Услуга по обработке защищаемой информации.

Каждый из элементов сервисов может быть самостоятельной услугой, а может входить в портфель услуг, предоставляемых поставщиком одним чехом. Посмотрим, из чего состоят те или иные услуги.

УПРАВЛЕНЧЕСКИЕ СЕРВИСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Услуга по организации (налаживанию) процесса обеспечения безопасности информации (БИ) является комплексной, состоящей из множества



— Вы правда, что ли, всё-всё за меня делать будете?
— Ага!

элементов и рассчитана на среднесрочное сотрудничество поставщика услуг с заказчиком услуг. Услуга применяется, как правило, когда требуется усовершенствовать имеющуюся систему обеспечения безопасности информации либо повысить уровень зрелости к обеспечению безопасности информации, а заказчик услуг не имеет работников требуемого уровня компетенции или такие работники заняты на выполнении других ответственных задач. В ходе оказания данной услуги, поставщик услуг на основе проведения независимой оценки состояния обеспечения безопасности информации у заказчика услуг или изучения результатов аналогичных оценок, проведенных ранее собственными силами заказчика или с привлечением им подрядчиков, формирует оптимальный проект (!) плана организации процесса обеспечения безопасности информации, определяет критерии (метрики) оценки эффективности принимаемых управленческих решений по обеспечению безопасности информации, и, используя собственные ресурсы, налаживает все процессы обеспечения безопасности информации у заказчика. Услуга включает в себя полностью или частично:

- ♦ оценку угроз и рисков безопасности информации;
- ♦ оценку уровня зрелости организации к обеспечению БИ;
- ♦ выбор уровня защищенности ИС;
- ♦ разработку плана обеспечения БИ;
- ♦ разработку метрик оценки эффективности БИ;
- ♦ разработку процедуры планирования обеспечения БИ;
- ♦ разработку процедур контроля состояния БИ;
- ♦ разработку процедур отчетности о состоянии БИ;
- ♦ разработку процедуры обработки инцидентов БИ;
- ♦ разработку процедуры восстановления состояния БИ после прерывания.

Перечень указанных элементов услуги не является окончательным и за-

висит от конкретных потребностей заказчика услуг и уровня ее зрелости к обеспечению безопасности информации.

Еще раз обратим внимание, что поставщик услуг только подготавливает и обосновывает решение по обеспечению безопасности информации, а само решение принимается руководством заказчика и претворяется в жизнь после его одобрения.

Услуга по разработке (пересмотру) документов, определяющих политику безопасности информации, также является комплексной и рассчитана на периодическое краткосрочное сотрудничество поставщика услуг и заказчика. Услуга применяется на этапе формирования системы обеспечения безопасности информации или с определенной периодичностью, установленной для пересмотра документов, определяющих политику обеспечения безопасности информации при отсутствии необходимых компетенций у работников заказчика услуг либо в случае возможного нарушения основных процессов обеспечения безопасности информации заказчика услуг за счет отвлечения штатных работников для пересмотра документов. Услуга включает в себя полностью или частично:

- ♦ разработку документов стратегического планирования обеспечения БИ;
- ♦ разработку документов оперативного управления обеспечением БИ;
- ♦ разработку документов текущего планирования обеспечения БИ;
- ♦ разработку регламентов выполнения процедур обеспечения БИ;

♦ разработку методик оценки и управления рисками БИ;

♦ разработку плана ликвидации нештатных ситуаций.

Перечень указанных элементов услуги также не является окончательным и зависит от конкретных потребностей заказчика, принятой у него системы организационно-нормативных документов и локальных нормативных актов и уровня ее зрелости к обеспечению безопасности информации.

При оказании услуги по разработке (пересмотру) документов поставщик услуги может содействовать заказчику в анализе существующих и разработке новых документов, определяющих политику безопасности информации, внутренних (корпоративных) стандартов, руководящих принципов и процедур. При этом, полномочия по утверждению данных документов, введению их в действие и ответственность за принятые решения остаются прерогативой заказчика.

Услуга по управлению рисками безопасности информации рассчитана на среднесрочное или долгосрочное сотрудничество поставщика услуг с заказчиком. Услуга применяется при уже сформированной системе обеспечения безопасности информации, когда у заказчика отсутствуют необходимые ресурсы для своевременного мониторинга рисков безопасности информации или на начальном этапе, когда работники заказчика еще не достигли требуемого уровня компетенции по управлению такими рисками и предполагает:

- ♦ разработку Руководства по управлению рисками безопасности информации;

Еще раз обратим внимание, что поставщик услуг только подготавливает и обосновывает решение по обеспечению безопасности информации, а само решение принимается руководством заказчика и претворяется в жизнь после его одобрения

- ♦ оперативное управление рисками и выработку рекомендаций по их снижению;
- ♦ проведение оценки рисков безопасности информации;
- ♦ разработку плана по снижению рисков информации.

При оказании услуги по управлению рисками безопасности информации поставщики услуг могут содействовать заказчикам в организации процедуры управления рисками, выполнению необходимых аналитических и экономических расчетов и выработке на их основе рекомендаций по снижению рисков. При этом заказчик услуг всегда остается ответственным за принятые решения по управлению рисками. В случае, если заказчик услуг уже имеет программу по управлению рисками безопасности информации, данная услуга, как правило, сводится к аудиту такой программы на предмет ее эффективности.

Услуга по разработке архитектуры безопасности информации относится к процессу подготовки решения по стратегическому планированию и развитию инфраструктуры безопасности информации. Услуга применяется на этапе проектирования и создания системы обеспечения безопасности информации и обуславливается необходимостью наличия специальных лицензий на выполнение работ по проектированию защищенных информационных систем, а также большими затратами по времени и привлечением квалифицированных ресурсов. Услуга носит разовый (но продолжительный) характер и предполагает:

- ♦ сбор необходимых исходных данных, инвентаризацию ресурсов и процессов БИ;
- ♦ определение бизнес-потребностей в обеспечении безопасности информации;
- ♦ определение функциональных требований к системе обеспечения безопасности;
- ♦ инвентаризацию и оценку технологий, которые позволят обеспечить БИ;

Услуга повышения осведомленности (обучения) персонала организации может носить как среднесрочный, так и периодический краткосрочный характер

- ♦ разработку методики выбора решений по обеспечению БИ;
- ♦ разработку и защиту проекта архитектуры системы БИ;
- ♦ разработку системы контроля (мониторинга) состояния БИ.

При оказании услуги по разработке архитектуры безопасности информации поставщики услуг могут содействовать заказчикам услуг в выполнении необходимых аналитических и экономических расчетов и выработке на их основе рекомендаций. При этом заказчик остается ответственным за принятые решения по выбору архитектуры безопасности информации на основе представленных рекомендаций.

ОПЕРАЦИОННЫЕ СЕРВИСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Услуга повышения осведомленности (обучения) персонала организации может носить как среднесрочный, так и периодический краткосрочный характер. Услуга применяется при уже сформированной системе обеспечения безопасности информации и обуславливается необходимостью владения специальными методиками обучения и развития навыков, наличия опыта слаживания коллектива, глубокого знания теоретических основ обеспечения безопасности информации и предполагает:

- ♦ разработку индивидуальных программ обучения работников основам обеспечения БИ;
- ♦ проведение тренингов, семинаров, воркшопов с работниками;
- ♦ обучение применению конкретных средств защиты;
- ♦ проведение периодических инструктажей работников по вопросам обеспечения БИ;

- ♦ подготовку рекомендаций по совершенствованию системы подготовки работников.

Услуга управления безопасностью информации относится к долгосрочным услугам и направлена на создание эффективного механизма управления процессами обеспечения безопасности информации при минимальных затратах на содержание обслуживающего персонала. Услуга основана на необходимости проведения достаточно сложной и квалифицированной работы по определению взаимосвязи (корреляции) между разрозненными событиями безопасности информации и выявлению возникающих событий, влияющих на ее состояние, а также выработки правил контроля за работоспособностью средств защиты информации. Услуга предполагает разработку регламентов устранения инцидентов и разделения полномочий по обработке инцидентов с передачей функций контроля и первичной аналитической обработки поставщику услуг, а также передачей ему прав управления (администрирования) средствами защиты информации. Услуга включает в себя:

- ♦ анализ возможных инцидентов и определение взаимосвязи событий;
- ♦ формирование базы решающих правил для обнаружения событий БИ;
- ♦ контроль (мониторинг) установленных безопасных конфигураций ИС и настроек СЗИ;
- ♦ администрирование средств защиты информации;
- ♦ консультационно-юридическую поддержку процессов обеспечения БИ.

Услуга расследования инцидентов безопасности информации (форензика) является эпизодической или может носить долговременный характер

(абонентское обслуживание). Услуга основана на необходимости наличия глубоких компетенций в юридической и технологической областях, а также анализа существующей судебной практики. Услуга требует использования специального программного обеспечения для сбора, анализа и фиксации данных об инциденте и предполагает:

- ♦ восстановление хронологии событий при инциденте;
- ♦ обнаружение используемых инструментов совершения противоправных действий;
- ♦ сбор и фиксацию доказательной базы по инциденту;
- ♦ установление источника инцидента;
- ♦ оценку масштаба произведенных действий и возможных последствий;
- ♦ подготовку рекомендаций по устранению инцидента и недопущению его в дальнейшем;
- ♦ установление виновного и причин его действий.

При оказании услуги расследования инцидентов, поставщик услуги может оказывать содействие заказчику услуги в юридическом оформлении ре-

зультатов расследования для передачи в компетентные органы, проведении независимых и судебных криминалистических экспертиз.

Услуга технического обслуживания средств защиты информации является среднесрочной или долгосрочной. Услуга обуславливается необходимостью наличия специальных лицензий на выполнение работ по техническому обслуживанию (например, для СКЗИ), отсутствием у заказчика работников требуемого уровня компетенции или, когда такие работники заняты на выполнении других ответственных задач. Состав услуги определяется текущими потребностями заказчика и составом применяемых средств защиты информации.

ТЕХНОЛОГИЧЕСКИЕ СЕРВИСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Услуга по реализации мер защиты является, как правило, долгосрочной и применяется при использовании арендуемой инфраструктуры для размещения информационной системы или передаче наиболее ресурсоемких функций обеспечения безопасности информа-

ции поставщику услуг. Такая услуга может быть оказана в различных комбинациях элементов услуги, предполагающих управление:

- ♦ средствами межсетевого экранирования ИС;
- ♦ средствами обнаружения вторжений в ИС;
- ♦ средствами защиты от DDoS-атак;
- ♦ средствами контентной фильтрации электронной почты;
- ♦ средствами защиты Web-приложений;
- ♦ средствами антивирусной защиты;
- ♦ средствами сбора и обработки информации об инцидентах;
- ♦ системами идентификации и аутентификации пользователей.

Услуга требует обязательной разработки регламентов взаимодействия поставщика услуг и заказчика, определения параметров передаваемых функций безопасности информации, определения порядка контроля за исполнением функций безопасности информации со стороны заказчика.

Услуга по предоставлению защищенной инфраструктуры для ИС также носит долгосрочный характер и характерна при использовании (аренде) инфраструктуры для размещения информационной системы или ее элементов в ЦОД или при аренде элементов инфраструктуры у поставщиков услуг. Она предполагает предоставление в пользование заказчику:

- ♦ инфраструктуры защищенной электронной почты;
- ♦ защищенных каналов связи;
- ♦ инфраструктуры открытых ключей;
- ♦ защищенного сегмента инфраструктуры ИС в ЦОД.

Перечень указанных элементов услуги не является окончательным и зависит от конкретных потребностей заказчика услуг и имеющейся у него инфраструктуры. Услуга требует обязательного подтверждения со стороны независимой экспертной организации возможности предоставления защищенной инфраструктуры поставщиком



услуг, разработки регламентов взаимодействия поставщика услуг и заказчика, определения параметров функций безопасности информации, реализуемых предоставляемой инфраструктурой и порядка контроля за исполнением функций безопасности информации со стороны заказчика.

Услуги по оценке безопасности продуктов и ИС могут носить как разовый (эпизодический), так и постоянный (периодический) характер. Применимость услуги обуславливается сложностью и трудоемкостью процедур оценки безопасности продуктов и ИС, необходимостью наличия специализированного стендового оборудования, методик и квалифицированного персонала. Услуга применяется как на этапе создания (модернизации) системы обеспечения безопасности информации, так и при периодических оценках соответствия информационной системы установленным требованиям безопасности информации. Услуга предполагает:

- ♦ проведение периодического анализа уязвимостей и тестирование ИС;
- ♦ проведение контроля безопасности кода программного обеспечения;
- ♦ проведение сертификации средств защиты информации;
- ♦ проведение периодической оценки соответствия ИС требованиям по БИ.

Услуга по безопасной разработке прикладного программного обеспечения предполагает не только разработку программного обеспечения, но и его поддержку в ходе эксплуатации, устранение выявленных уязвимостей, совершенствование механизмов защиты, применяемых в программном обеспечении. Применимость услуги обуславливается ресурсоемкостью процесса разработки прикладного программного обеспечения, необходимостью глубокого знания стандартов и методик разработки безопасного программного обеспечения, проведения значительного объема тестовых испытаний по поиску и устранению уязвимостей. Услуга применя-



— Замесить и нарубить!

ется на этапе создания (модернизации) информационной системы.

Услуга по обработке защищаемой информации носит долгосрочных характер и применяется в случае отсутствия у заказчика необходимой инфраструктуры и специалистов и предполагает передачу поставщику услуг всего цикла обработки информации. Данная услуга наиболее характерна для малых и микро-организаций. При оказании данной услуги заказчик услуг, передавая весь процесс обработки информации поставщику услуг, остается ответственным за обеспечение безопасности информации. Данная услуга связана с допуском работников поставщика услуг к защищаемой информации в полном объеме и требует тщательного докумен-

тирования необходимых требований по обеспечению безопасности информации и порядка взаимодействия сторон.

ЧАСТЬ 3. ВОРОХ ДОКУМЕНТОВ

Привлекая поставщика услуг, заказчик пускает его в свою жизнь, встраивает в свои бизнес-процессы. И зачастую отказаться от услуг поставщика бывает сложнее, чем начать отношения с ним. Поэтому правила игры надо выстраивать еще на берегу, до того, как приступить к потреблению благ от поставщика. Здесь важно все грамотно юридически оформить, чтобы в дальнейшем не было мучительно больно за бесцельно потраченные деньги. Поэтому и требуется целый ворох правильных документов, охватывающий

Привлекая поставщика услуг, заказчик пускает его в свою жизнь, встраивает в свои бизнес-процессы. И зачастую отказаться от услуг поставщика бывает сложнее, чем начать отношения с ним

Существенными условиями договора возмездного оказания услуг являются предмет договора (осуществление определенных действий или определенной деятельности) и цена

все аспекты дальнейшего сотрудничества между поставщиком и заказчиком услуг. Пакет документов при передаче функций (процессов) обеспечения безопасности информации поставщику услуг должен включать в себя:

- ♦ договор с поставщиком услуг;
- ♦ соглашение об уровне предоставления услуг (SLA);
- ♦ соглашение о конфиденциальности (NDA);
- ♦ требования по безопасности информации (для отдельных видов услуг);
- ♦ поручение на обработку защищаемой информации (для отдельных видов услуг);
- ♦ регламент взаимодействия.

Договор с поставщиком услуг

Договор с поставщиком услуг по своей сути является комплексным договором, но в своей основе относится к договорам возмездного оказания услуг, при котором ценностью для заказчика являются сами действия исполнителя в ходе оказания услуги как процесс, а не достижение поставщиком определенного результата. Такой договор оформляется в соответствии с требованиями ст. 779 ГК РФ, которая предусматривает совершение определенных действий или осуществление определенной деятельности поставщиком услуг. Исключение составляет договор на передачу обработки защищаемой информации поставщику услуг, который заключается как договор поручения в соответствии со ст. 971 ГК РФ.

Существенными условиями договора возмездного оказания услуг явля-

ются предмет договора (осуществление определенных действий или определенной деятельности) и цена. В договоре должны быть четко указаны перечень услуг и конкретные действия, которые поставщик услуг обязан совершить для заказчика. Можно, конечно, не указывать в договоре конкретный объем услуг, если он определяется в дополнительных соглашениях между сторонами. В договоре, в зависимости от оказываемых услуг, также должно быть отражено:

- ♦ обязанность поставщика услуг оказывать услуги личным исполнением;
- ♦ уровень качества оказываемых услуг;
- ♦ обязанность обеспечения безопасности информации поставщиком услуг;
- ♦ обязанность поставщика услуг не раскрывать третьим лицам и не распространять защищаемую информацию;
- ♦ обязанность поставщика услуг принять технические и организационные меры защиты в соответствии с требованиями заказчика услуг;
- ♦ обязанность поставщика услуг провести оценку эффективности принятых мер защиты;
- ♦ обязанность поставщика услуг соблюдать согласованные показатели качества услуг;
- ♦ право и возможность оператора осуществлять проверку (контроль) принятых мер защиты (аудита безопасности), в том числе с привлечением третьей независимой стороны;
- ♦ право оператора осуществлять проверку (оценку) качества выполнения услуг;

♦ санкции за нарушение мер защиты и за невыполнение согласованных ключевых параметров качества услуг и порядок возмещения ущерба;

♦ состав услуг, поддерживаемых поставщиком услуг в случае возникновения чрезвычайных ситуаций;

♦ порядок приемки оказанных услуг.

Чтобы облегчить себе жизнь в дальнейшем, при подготовке договора надо стремиться к включению в него положений, обеспечивающих полную компенсацию ущерба от нарушения мер защиты и невыполнения согласованных параметров качества, включая репутационный и моральный ущерб, без обращения в суд.

В договоре также целесообразно указать услуги (сервисы), которые будут поддерживаться поставщиком услуг в случае возникновения чрезвычайных ситуаций, а также возможность проведения независимого аудита обеспечения безопасности информации со стороны поставщика услуг третьей независимой стороной.

Обычно поставщик услуг предоставляет некоторый период тестирования своей услуги для принятия окончательного решения о ее предоставлении. Но если перед заключением договора этап тестирования предоставляемой услуги не проводится, в договор надо включить положение, по которому в течение определенного периода услуги оказываются бесплатно, и заказчик в течение этого периода вправе расторгнуть договор без каких-либо санкций и обязательств.

Все положения договора возмездного оказания услуг должны быть согласованы сторонами. К договору могут быть приложены в качестве неотъемлемой части договора остальные документы из состава пакета договорных документов.

(Окончание в следующем номере)

В оформлении статьи использованы иллюстрации А. М. Савченко из книги «Вовка в Тридевятом царстве» (издательство «Астрель», 2005 год) и кадры из мультфильма «Вовка в Тридевятом царстве» режиссёра Бориса Степанцева (Союзмультфильм, 1965 г.).



Сергей НЕЙГЕР

сотрудник отдела
компании «Перспективный мониторинг»

Поставщики услуг обеспечения безопасности информации и их потенциальные заказчики уже много лет до хрипоты спорят между собой: что дешевле / технологичнее / современнее — инсорсинг или аутсорсинг, что можно и что нельзя передавать на аутсорсинг, кто принимает решения и несёт за них ответственность?

Сергей Викторович и Артём Михайлович говорят о доверии между заказчиком и провайдером аутсорсинга и приводят конкретные способы выстроить это доверие. Эти факторы доверия должны иметь не меньшее значение при выборе провайдера, чем целевой уровень защищённости информационных ресурсов или экономические преимущества от сотрудничества.

Предположим, что стороны долго присматривались друг к другу и, наконец-то, договорились. Тогда провайдер и заказчик должны обеспечить две составляющие передачи функций обеспечения безопасности информации на аутсорсинг — техническую и организационную. К технической составляющей относятся аппаратная и программная части: оборудование, программное обеспечение и лицензии. К организационной — договор, соглашение об уровне предоставления услуг, соглашение

о конфиденциальности, требования по безопасности информации, регламенты взаимодействия.

Но также нельзя забывать про принципиальное решение о передаче функций ИБ на аутсорсинг — про волю заказчика. Можно передать функции, можно передать некоторые риски, можно передать даже часть ответственности — но не само решение.

Поясню на примере. У нас в компании «Перспективный мониторинг» уже почти два года функционирует коммерческий Центр мониторинга. Мы постоянно контролируем ИБ-инфраструктуры нескольких организаций, собираем записи о событиях ИБ из различных источников и выявляем инциденты. Предположим, что мы зафиксировали инцидент — на одном из контролируемых хостов замечена активность вредоносного ПО. Сами по себе такие инциденты не очень «страшные», мы обычно классифицируем их как инциденты низкой критичности. Какие варианты действий есть у провайдера услуг безопасности? Первый вариант: дежурная смена SOCa сама проверяет хост, изолирует его, удаляет ВПО. Технологических препятствий для такого сценария нет, всё осуществимо. Второй вариант: дежурная смена оповещает заказчика об инциденте, готовит рекомендуемый план действий по реагированию для ИТ и ИБ специалистов заказчика (см. вариант 1) и контролирует поведение подозрительного узла.

SOC «Перспективного мониторинга» работает только по второму варианту. Мы оказываем услуги монито-

ринга по максимально безопасному сценарию, в котором мы сами не можем даже случайно нарушить доступность сервисов. Мы только смотрим журналы ПО и оборудования и не «лезем руками» в контролируемую информационную систему, а значит у нас нет доступа к конфиденциальной информации. А у заказчика всегда остаётся право принять решение, использовать наши рекомендации по реагированию или нет. Благодаря такому подходу от наших услуг можно безопасно отказаться. Это очень важный момент, которому редко уделяется достаточно внимания на этапе начала сотрудничества. Мы делаем заказчика сильнее в противостоянии со злоумышленником, но без нас он слабым тоже не станет! Когда мы работаем вместе, заказчик видит те же инструменты и ту же отчётность, что и мы, и может при желании обучать собственную первую линию мониторинга. В таком случае за нами остаётся вторая линия, разработка правил и средств мониторинга, помощь в расследовании инцидентов.

Хочется поблагодарить авторов эссе за то, что они поделились своим опытом построения СОБИ с привлечением аутсорсеров, колоссальную исследовательскую работу и систематизацию нормативно-правовых актов и публикаций. Этот номер BIS Journal станет настольным пособием и для провайдеров услуг ИБ, и для заказчиков.

Можно передать функции, можно передать некоторые риски, можно передать даже часть ответственности — но не само решение

СОС'И РОССИИ



Александр БОДРИК
CISA, CCSK, ITIL
Expert

ОХОТНИКИ БЛИЗКО!

Вместо предисловия

Последние несколько лет я ежедневно структурирую проекты по инвестициям в ИБ на десятки и сотни миллионов рублей. IDM, SIEM, Anti-Fraud, GRC, IPS — технологии меняются, а подспудное ощущение, что что-то мы все делаем не так, остается. Типовая сделка в 20–30 миллионов рублей сопровождается буквально нулевым вниманием к человеческому капиталу. Стандартная практика — создание инструкций администратора и пользователя, иногда обучение и описание релевантных уже существующих процессов. Все!

Итоговый процент инвестиций в человеческий капитал в проекте редко достигает и 1%. Большинство клиентов понимает проблему, но почти ничего не может поделать. Руководители ИБ представительств западных корпораций и нефтегазовых лидеров мира, крупнейшие банки и оборонные концерны, ведущие ритейлеры и строители — все страдают от невозможности инвестировать в человеческий капитал хотя бы пропорционально технологиям.

Все понимают: платить справедливую мировую стоимость инженера «политически» опасно. Во многих корпорациях его компенсация будет сродни компенсации топ-менеджера. Вот и происходят «положные внедрения», когда инвестиции происходят в «полку», где лежат без движения самые разные продукты — примерно как мобилизационный запас на случай войны. Вот взламывают — развернем, а до этого — ну его.

Однако в рамках растущей тематики СОС традиционный подход может быть губителен. Ориентированные на блокирование средства защиты (условный межсетевой экран) еще мо-

гут быть один раз внедрены и время от времени немного настраиваться, но не современные средства детектирования и реагирования на инциденты. Хотя каждому понятно: чтобы быть эффективным, СОС должен все время эволюционировать, адаптировать технологии, процессы и компетенции персонала к изменяющемуся ландшафту угроз и внутренней инфраструктуре.

Растущая тема СОС дает и шанс просто сохранить компетенции. На расстоянии вытянутой руки, за прозрачной стеклянной стеной государственной границы находятся Сингапур, Гонконг, Германия, Великобритания, США, где сопоставимого качества эксперт по технологиям ИБ имеет ставки в 3–5 (вплоть до 10) тысяч долларов в месяц — выше чем даже в крупнейших корпорациях и технологических компаниях России. Эта прозрачная стена готова рухнуть от усилий всего нескольких кадровых агентств, ведь Сингапур, Гонконг и Германия — это еще и мягкий миграционный режим для ИТ-специалистов, десятки высокооплачиваемых вакансий и понятная перспектива появления еще сотен.

Возможно, концентрация корпоративных ресурсов под флагом СОС (создание максимально комфортных, эффективных и прозрачных для персонала процессов и организационных моделей, рост инвестиций в человеческий капитал) — это последний шанс укрепить кадровые рубежи перед тем, как наши заграничные партнеры начнут полномасштабную охоту за головами российских технологических талантов в сфере ИБ.

ЕСТЬ ПРОБЛЕМЫ. И НЕ БУДЕМ ЭТОГО СКРЫВАТЬ!

Почти 20 лет назад — 2 ноября 1988 года — состоящий всего из 99 строк кода червь Морриса (получивший прозвище Великий Червь) заразил 6 000 компьютеров ARPANET, создав существенные проблемы более чем десятку университетов и корпораций. Отразив атаку и «вылечив» компьютеры, организация, создавшая ARPANET, — Агентство перспективных оборонных исследований (DARPA) вместе с Университетом Карнеги-Меллон создала компьютерную команду реагирования на чрезвычайные ситуации (CERT — Computer Emergency Response Team), ставшую фактически первым Security Operations Center.

Перед первым SOC были поставлены задачи реагирования на инциденты кибербезопасности, проведения исследований, сбор информации об уязвимостях и повышения осведомленности пользователей о новейших угрозах. Со временем, ввиду интеграции разрозненных инфраструктур и оцифровки бизнес-процессов предприятий, задачи реагирования на инциденты (управления инцидентами) и управления уязвимостями многократно укрупнились, разветвились и стали краеугольными камнями понятия security operations.

СЕРВИСЫ И ПОТРЕБИТЕЛИ СЕРВИСОВ SOC

С годами обязанности SOC расширялись, и CERT Карнеги-Меллон выделяет уже 17 сервисов ИБ (рисунок 1).

Российские SOC на практике предоставляют 4 базовые услуги внешним или внутренним потребителям:

1. Поддержка средств защиты (в первую очередь сенсоров).

2. Мониторинг кибератак и реагирование на инциденты (управление инцидентами в узком смысле).

3. Сканирование и контроль закрытия уязвимостей инфраструктур и ПО (управление уязвимостями в узком смысле).

4. Киберразведка (мониторинг уязвимостей, последних атак как минимум на основе публично доступной информации от ключевых ИБ-вендоров).

Цикл запуска сервиса SOC возможно поделить на ряд этапов (таблица 1).

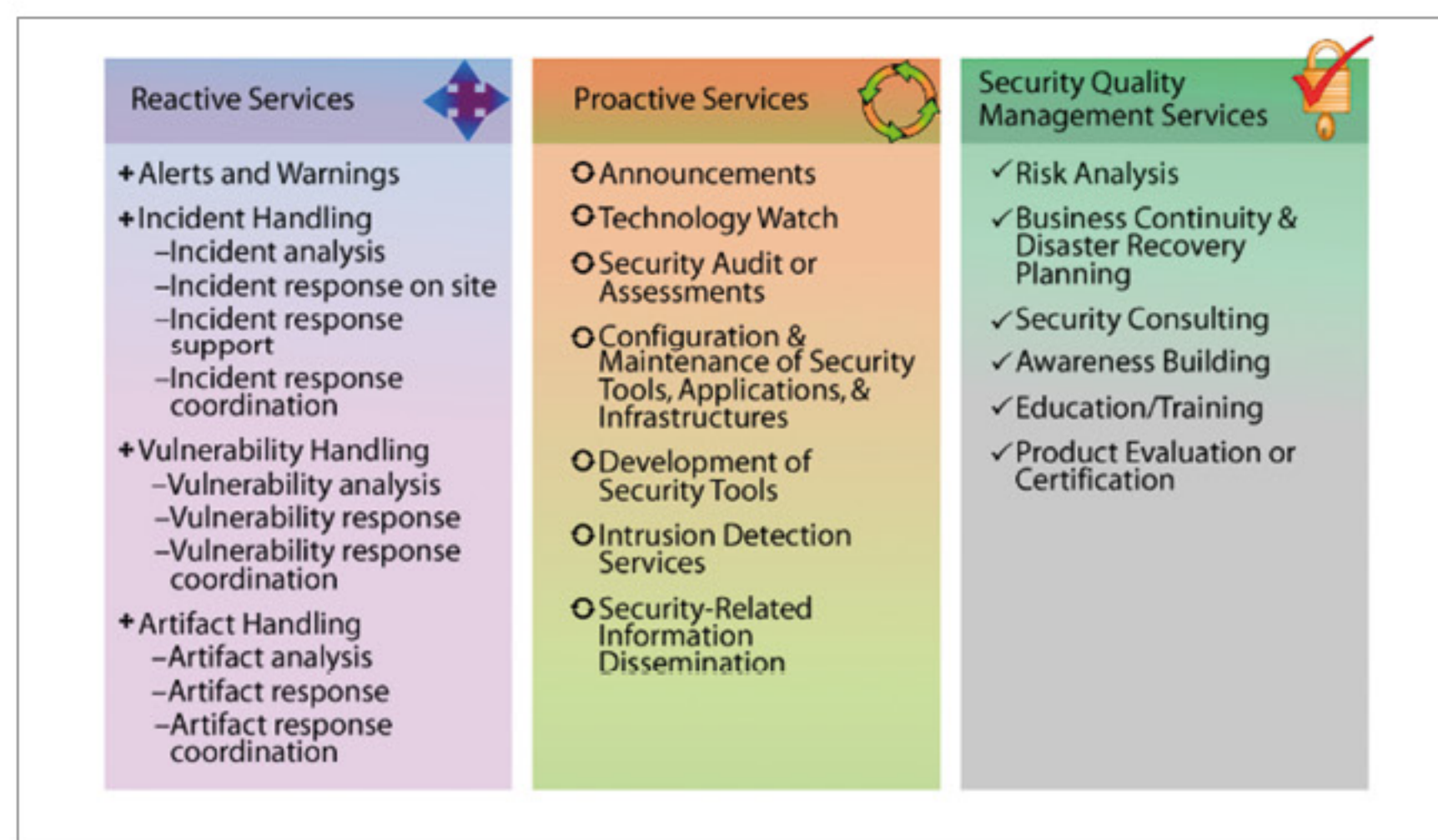


Рисунок 1. Сервисы SOC по версии CERT Карнеги-Меллон

№	Этап	Результаты	Предыдущий этап	Следующий этап
1	Обследование области мониторинга	База знаний (Wiki\CMDB)	Нет	2
2	Установка точек контроля	Возможность мониторинга	1, 5	
3	Мониторинг\Поддержка	Инциденты выявлены (IDS, SIEM etc) и зарегистрированы (SD\Workflow)	2, 5	
4	Реагирование	Ущерб минимизирован, Отчетность по инцидентам	3	
5	Совершенствование деятельности	Новые кейсы и практики введены в работу	3, 4	

Таблица 1. Этапы запуска нового сервиса SOC

Корпорации создают или заказывают сервисы SOC по заказу одной или нескольких заинтересованных сторон (потребителей сервисов). Таких типовых заинтересованных сторон 5:

1. Генеральный директор. Цель — защита стоимости акций, репутации, капитала, интеллектуальной собственности и доходов компании.
2. Финансовый директор. Цель — соответствие требованиям (например, SOX).
3. ИТ-директор. Цель — обеспечение непрерывности предоставления ИТ-услуг.
4. Директор по безопасности. Цель — обеспечение сохранности корпоративных активов.
5. Региональный менеджмент. Цель — получение доступа к корпоративным централизованным ИТ-сервисам (что иногда невозможно без заказа централизованных сервисов SOC).

Иногда SOC создается как часть проекта по централизации функций поддержки бизнеса, т.е. в целях снижения затрат. Его функции могли выполнять отделы ИБ во всех регионах и странах присутствия корпорации, а теперь за счет централизации будет возможно повышение качества и снижение удельных затрат. Кстати, более 75% компаний из списка Fortune 500 (а в нефтяной отрасли 90%) уже реализовали у себя программы централизации предоставления услуг. Из публичных российских примеров в части информационной безопасности, это: Росатом, Роснефть, Газпром, Сбербанк, Норникель, Северсталь. Однако, стоит отметить, что степень централизации может быть разной. Где-то, как в одном из дивизионов нефтегазового чемпиона, реализован единообразный SOC-сервис на 20 000 рабочих станций, где-то, как в федеральном госоргане, централизована только часть функций, и полная централизация невозможна ввиду застарелого конфликта ИТ и ИБ — всегда будут нужны специалисты ИБ на местах, поскольку ИТ не соглашается взять на себя даже самые мелкие задачи.

Внешними клиентами коммерческих SOC остаются 3 основных типа организаций:

1. Крупные глобальные организации в рамках проектов по аутсорсингу функций поддержки бизнеса.
2. Организации в регулируемых сферах бизнеса — публичные, платежные организации (SOX, PCI DSS, etc.).
3. Организации среднего размера, масштаб которых делает избыточным найм, содержание и удержание квалифицированного персонала SOC.

ОРГАНИЗАЦИОННАЯ МОДЕЛЬ SOC

Определив тип SOC (внешний\внутренний), портфель и заказчиков сервисов, становятся понятны зона ответственности и предпосылки к формированию организационной структуры, географической модели предоставления сервисов, стандартов компетенций персонала, программ набора и удержания персонала, — все то, что в совокупности именуется операционной\организационной моделью SOC, позволяющей стабильно предоставлять сервисы SOC заказчикам с предсказуемым качеством и объемом.

Рассмотрим несколько примеров крупных SOC. Ввиду специфики нашей отрасли только один SOC согласился выступить «с открытым забралом» — это Solar Security. Были направлены запросы и двум другим коммерческим SOC (Лаборатория Касперского и Позитив Технолоджис), но они не согласовали визит.

Пример 1. Глобальный SOC, сфокусированный на предоставлении сервиса киберразведки внешним заказчикам. Присутствие в 12 странах на всех континентах. Организационная структура основного бизнеса типа «спрут» разделена на 4 блока — Customer Care (отношения с потребителями), Global Analytics (аналитики и служба контроля качества), Special Operations (технические сервисы — форензик, реверс-инжиниринг, реагирование на инциденты), Global Intelligence (сбор информации). Первые 3 блока в итоге были централизованы в головной стране, блок Global Intelligence состоял из локальных Risk Management Centers + центр технической компетенции в европейской штаб-квартире. Организационная структура Risk Management Center — «кольцо» — все делают все, но есть и зачатки специализации: кто-

Более 75% компаний из списка Fortune 500 (а в нефтяной отрасли 90%) уже реализовали у себя программы централизации предоставления услуг

то специализируется на уязвимостях, кто-то — на аналитике, кто-то — на fraud intelligence. Источники персонала — студенты, национальные CERTы, отставники правоохранительных органов и спецслужб.

Пример 2. Топовая нефтегазовая корпорация России (А). SOC предоставляет сервисы мониторинга атак, уязвимостей и поддержки средств защиты для всех российских предприятий (20 000 ПК). Организационная структура SOC — «двойной спрут» — методологическое ядро и служба контроля качества в Москве, операционное ядро в Рязани, технический сервис сперва в Рязани, потом в Саратове (вслед за наличием редкой компетенции), задачи реагирования на инциденты на местах выполняли службы ИБ-предприятий. Организационная структура операционного ядра — «паутина» — по каждой значимой системе ИБ работало 2 человека, так же 2 человека решали вопросы отчетности, управления, мотивации и найма. Источник персонала — студенты, системные и сетевые администраторы с рынка. Кстати, рядом с «классическим» SOC работал распределенный центр мониторинга бизнес-транзакций, фактически «антифрод-SOC» (контроль фрод-рисков в продажах нефтепродуктов на АЗК) — численность персонала, организационная структура и географическое распределение работ было в целом аналогичным.

Пример 3. Топовый телеком оператор России. SOC предоставляет сервисы мониторинга атак и уязвимостей в рамках SOX-критичной области. Весь SOC расположен в Москве, организационная структура — «пирамида» (аналитики 1-го уровня приоритезируют инциденты и решают что могут, иначе эскалируют, аналитики 2-го уровня решают инциденты, аналитики 3-го уровня вносят изменения в правила мониторинга). Задачи реагирования на инциденты на местах выполняли менеджеры по ИБ макрорегионов. Технический сервис и служба контроля качества отсутствуют. Источник персонала — повышение квалификации существующих специалистов службы ИБ, найм с рынка.

Пример 4. Топовая нефтегазовая корпорация России (Б). SOC предоставляет сервисы мониторинга атак и поддержки средств защиты

Ввиду специфики нашей отрасли только один SOC согласился выступить «с открытым забралом» — это Solar Security

в рамках московского сегмента инфраструктуры (до 6 000 ПК), региональная инфраструктура не входила в объем мониторинга. Технический сервис и служба контроля качества отсутствуют. Организационная структура простая, нет ярко выраженного разделения на аналитиков по уровням, задачи реагирования на инциденты на местах закрывались службами ИБ предприятий. Источник персонала — студенты, повышение квалификации существующих специалистов службы ИБ, найм с рынка.

Пример 5. Топовый банк России. SOCи предоставляют сервисы поддержки средств защиты, мониторинга атак и уязвимостей в рамках московского и региональных сегментов инфраструктуры. Московский и региональные SOCи оперируют фактически самостоятельно, даже не ведут полноценную единую техническую политику. Технический сервис и служба контроля качества отсутствуют, но привлекается на аутсорсинг технический сервис для помощи в расследованиях хищений со счетов клиентов (ДБО и т.п.). Организационная структура простая, нет ярко выраженного разделения на аналитиков по уровням, задачи реагирования на инциденты на местах закрывались службами ИБ подразделений филиалов. Источники персонала — не предоставляется возможным определить, SOCи формируются стихийно.

Пример 6. Коммерческий SOC Solar Security. Предоставляет сервис мониторинга атак и уязвимостей для внешних клиентов (из публичных — Тинькофф банк, СТС Медиа). Организационная структура SOC — распределенные на Москву и Нижний Новгород «песочные часы». Увеличено количество аналитиков 3-ей линии для более полного технического понимания инфраструктуры клиентов, аналитики 1-й линии расположены в Нижнем Новгороде, 3-ей — в Москве. Существуют технический сервис и служба контроля качества, задачи реагирования на инциденты у клиентов распределены между 3-ей линией и службами ИБ клиентов.

С точки зрения лучших практик CERT (CERT Карнеги-Меллон, Европейского агентства по информационной и сетевой безопасности) организационная структура CERT должна начинаться с института triage officer (в переводе «распределяющий офицер»), который, обладая знаниями последних угроз, трендов и актуальных векторов атак, должен произвести первичную обработку каждого инцидента и определить, не является ли он «ложно положительным». Однако, на практике в российских и глобальных SOC эту функцию возлагают на 1-ю линию, иногда подпирая ее последующим ревью кейсов службой контроля качества (Пример 6).

На основе анализа вышеприведенных примеров возможно выделить ряд компонентов SOC, целесообразность которых необходимо рассмотреть при создании эффективного и полноценного подразделения:

1. Управленческий орган SOC для координации как рабочих процессов, так и критичных вопросов найма, оценки, мотивации и удержания персонала SOC.
2. Методологический блок SOC.
3. Операционное ядро SOC — 1-я линия (операторы), 2-я и 3-я — аналитики.
4. Дополнительные блоки SOC — технический сервис, институт службы контроля качества (может быть реализован силами аналитиков SOC).

ПОРТРЕТ АНАЛИТИКА SOC

Даже самые лучшие организационные практики не позволят построить устойчиво эффективный SOC без качественного человеческого капитала — сотрудников. Объединяющими различные SOC минимальными требованиями к операторам и аналитикам будут 3 профессиональных и 3 личных. Среди профессиональных — знания сетевой архитектуры и протоколов (стека TCP/IP и др.), знания UNIX (основы современных средств защиты) и знания используемых SOC средств защиты (IDS, FW, web proxy, AV). Среди личных — мотивация к обучению, стрессоустойчивость, склонность к командной работе.

Многие другие качества (знания ландшафта угроз, специфики корпоративных ландшафтов и процессов ИТ и ИБ, хакерских практик и утилит) тоже будут ценным подспорьем, но их возможно «добрать» в процессе работы.

Крупный SOC со штатом в десятки человек выводит на уровень оператора за 1,5 месяца, на уровень полноценного аналитика 2-й линии — за 1,5 года (данные Solar Security).

7 ОРГАНИЗАЦИОННЫХ ПРОБЛЕМ SOC

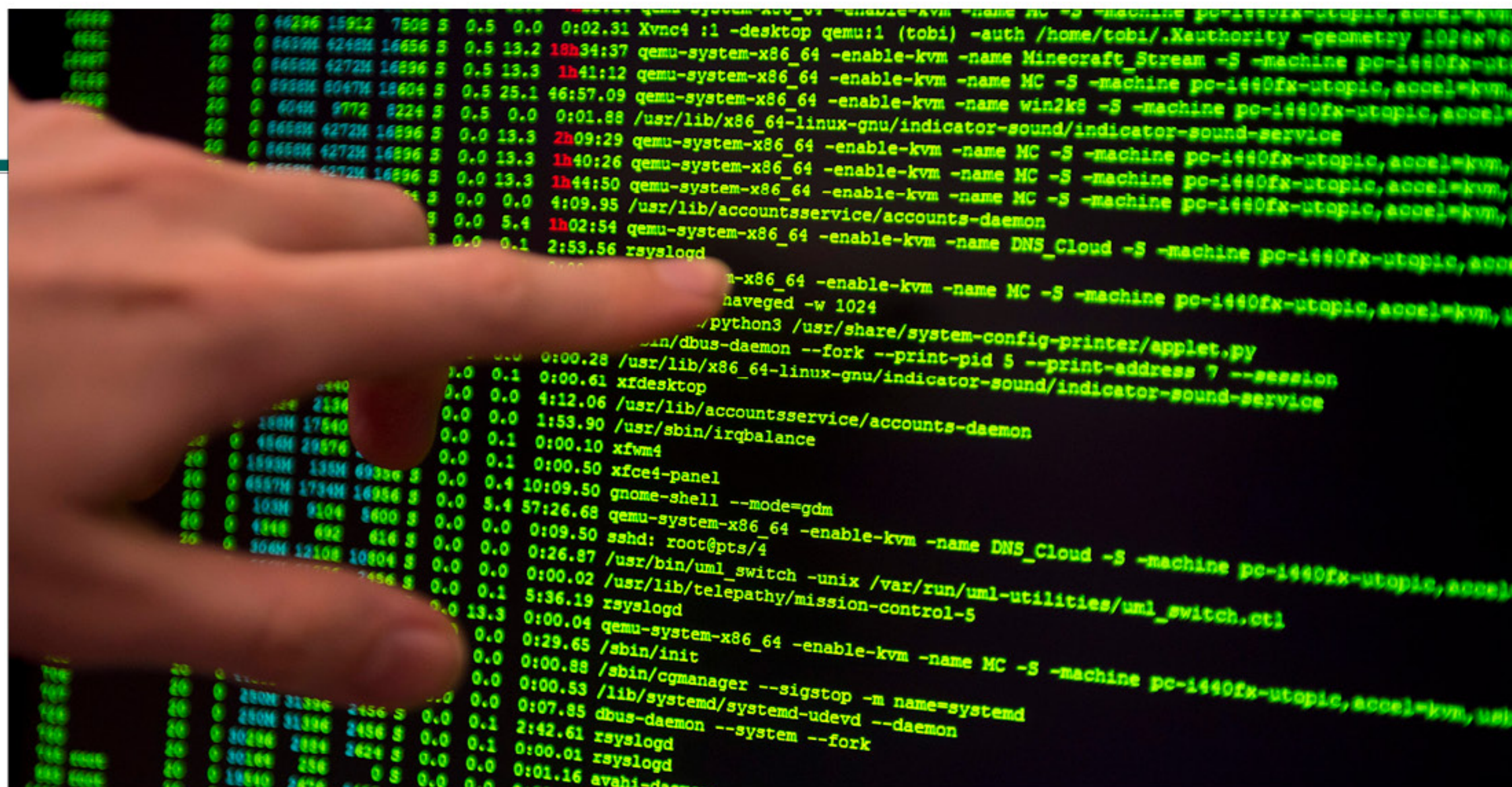
Руководители признаются, что даже в существующих годами крупнейших SOC с отстроенными процессами и успешной практикой, бывают и проблемы. Сколько и какие? 7 типовых описаны ниже:

1. Предопределенность решений культурной спецификой. В ряде организаций отсутствует рабочий диалог между ИТ и ИБ. Это является в невозможности поручить ИТ даже самые простые и небольшие по объёму задачи, а без этого сложно централизовать сервисы ИБ — сманеврировать, создав мощный SOC без увеличения штата. В каждом регионе России приходится держать локальных специалистов, размывая тем самым человеческий капитал службы ИБ по всей стране. Рецепт решения проблемы (из Примеров 2, 3) будет установление максимально возможных добрососедских отношений с коллегами из ИТ.

2. Отсутствие высококвалифицированных специалистов. Квалифицированных аналитиков SOC в стране всего несколько десятков, это штучные специалисты и иногда их просто негде взять. Рецепт решения проблемы (из Примеров 2,6) будет разработка стандартов компетенции должностей, запуск программ стажировок и привлечения студентов.

3. «Охота за головами». Начиная как минимум с 2008 года в России каждый год открывается либо существенно реорганизуется крупный корпоративный SOC. Процесс начинает приобретать лавинообразный характер. Подчеркну, что SOC в данном случае — это не просто SIEM и 2 аналитика, а полноценная организация с четкими целями, сервисами и заказчиками, полноценными процессами и практиками. Открывающиеся SOCи ведут активную «охоту за головами» из уже существующих. Рецепт

Крупный SOC со штатом в десятки человек выводит на уровень оператора за 1,5 месяца, на уровень полноценного аналитика 2-й линии — за 1,5 года



решения проблемы (из Примеров 2, 3, 5) будет повышение компенсации ключевым сотрудникам, выделение сотрудников SOC в отдельную ИТ\ИБ дочернюю компанию.

4. Текучка. Квалифицированные аналитики SOC могут применить свои знания и на других участках работы службы ИБ (в частности, несколько аналитиков из Примера 2 доросли до уровня директоров по ИБ) и являются востребованными на рынке труда. Дополнительный фактор риска — рутинная работа на 1-й линии, которая может просто наскучить специалистам. Рецепт решения проблемы (из Примеров 2, 6) — формирование и внедрение программы взаимодействия с вузами для формирования кадрового студенческого резерва.

5. Малая емкость рынка кадров. Открытие SOC в городах с малым количеством крупных предприятий и представительств федеральных корпораций может привести к вынужденной ориентации исключительно на студентов. Рецепт решения проблемы (из Примеров 4,5,6) — открывать SOC в крупных городах с развитыми университетскими сообществами — в Москве, Нижнем Новгороде, Казани, Новосибирске и т.д.

6. Слабая автоматизация. Слабую автоматизацию деятельности SOC в России можно назвать нормой. На одном из важных участков с ней точно проблемы — нет развитой SIEM, нет workflow системы, нет базы знаний\CMDB, нет sandbox решений или то, что есть, устаре-

ло и толком не поддерживается. Рецепты решения проблемы (из Примеров 2, 3) — использование «легких» open source решений (OTRS, ciscooo), использование скриптов, перенос рутинных операций в регионы с более низкими компенсациями.

7. Отсутствие ежегодного повышения квалификации. Инвестиции в обучение персонала SOC часто сдерживаются текучкой: «Вот мы их учим, а они все уходят». С другой стороны, а что будет, если не учить? Рецепты решения проблемы (из Примеров 2, 3, 6) — план развития персонала, стандарты компетенций (от какой точки до какой мы ведем сотрудника), обучение одного сотрудника с последующим трансфером знаний.

«Нет худа без добра» — классическая поговорка как нельзя более применима к текущему ландшафту угроз, когда участвовавшие инциденты выступают драйвером создания SOC. Они стимулируют не только создавать SOC, но и активно ориентироваться на результат — жестко тестировать новые подходы к управлению и организации SOC и служб ИБ в целом, пересматривать существующее историческое наследие в процессах и технологиях ИБ. Этот шанс может оказаться последним перед тем, как международные игроки и зарубежные партнеры кардинально изменят расстановку на российском кадровом ИБ-рынке.



Дмитрий КУЗНЕЦОВ
директор по методологии
и стандартизации
компании Positive
Technologies

BIS-КОММЕНТАРИЙ

SOC НА ЧЕТЫРЕХ КИТАХ

Когда начал развиваться рынок аутсорсинга ИБ, в ряде компаний и гос. ведомств появилась практика перекладывать функции ИБ на сервисные компании, а некоторые из них стали называться Security Operations Center (SOC). Деятельность таких стихийных SOC по своему содержанию и результативности мало отличалась от собственных подразделений ИБ компании, а стоила существенно дороже. Годы шли, опыт накапливался, и сегодня на рынке SOC сформировался определенный подход к их построению и функционированию.

Специализация. Сегодня уже не нужно «обеспечение ИБ вообще», бизнес требует решения определенных задач, которые не может решить самостоятельно. Банку требуется специализированный фрод-мониторинг, защита от компьютерных атак и расследование финансовых киберпреступлений, нефтеперерабатывающей компании — выявление хищений нефтепродуктов и защита от «очумелых ручек» собственных сотрудников, государственным ведомствам — предписанные указом Президента обнаружение, предупреждение и ликвидация последствий компьютерных атак. Это привело к появлению на рынке SOC игроков, специализирующихся на оказании определенного (пусть и небольшого) набора специализированных услуг, но зато разбирающихся в своей предметной области досконально.

Кооперация. Когда инженер сервисной компании приезжает на электроподстанцию, чтобы «правильно настроить функции безопасности», вряд ли его встретят хлебом-солью. Практика сформировала четкое разделение обязанностей между SOC и персоналом защищаемой системы: SOC формирует специфические требования к ее средствам защиты, обрабатывает данные регистрации событий, применяет собственные пассивные или «неинвазивные» инструменты, координирует действия при инцидентах, контролирует защищенность и т.п. Но все, что требует непосредственной работы с компонентами ИС, выполняет обслуживающий персонал.

В последнее время некоторые коммерческие, на первый взгляд конкурирующие, SOC наладили обмен полезной информацией друг с другом.

По результатам реагирования на принципиально новый инцидент SOC формирует индикаторы компрометации, сигнатуры для IDS, правила корреляции для SIEM — и зачастую публикует основные материалы в комьюнити или распространяет через подписку. Принцип обмена информацией хорошо зарекомендовал себя в индустрии антивирусных средств и в банковской сфере, его взяли на вооружение и государственные регуляторы, предусматривая кооперацию государственных и коммерческих SOC в рамках системы ГосСОПКА.

Автоматизация. Сервисный контракт предполагает, что в случае инцидента к вам выедет специалист SOC и будет разбираться с логами, используя привезенные с собой подручные средства? А вы уверены, что ваш подрядчик имеет опыт реагирования на инциденты? Современный SOC — это централизованный комплекс средств автоматизации, куда входят и средства мониторинга (IDS/IPS, сканеры уязвимостей, DPI, лог-коллекторы), средства анализа (SIEM, средства анализа приложений), и средства организации рабочего процесса. Если говорить о кибератаках, то на сегодняшний день уже определились требования к составу средств SOC, необходимых для противодействия кибератакам. Они находят отражение, например, в нормативных документах ФСТЭК, стандартах Банка России, проектах методических документов по функционированию ГосСОПКА.

Персонал. Автоматизация работы SOC и та самая кооперация позволяют держать персонал там, где он есть, а не там, где находится заказчик. Нужны грамотные специалисты первой линии с перспективой их перевода на позиции, требующие более высокой компетенции? В ВУЗах многих городов уже несколько лет ведется обучение студентов по специализированным программам в области кибербезопасности, в разработке которых принимают участие и профильные вендоры (именно для этого мы тратим ресурсы на Positive Education и соревнования CTF).

По большому счету в индустрии SOC не все так грустно, как пишет автор. Хотя, конечно же, этому рынку еще есть куда развиваться.



Кибербезопасность крупных организаций и предприятий

Комплексная платформа для защиты
крупных IT-инфраструктур и промышленных сред

- Контроль и защита рабочих мест
- Защита виртуальных сред
- Защита центров обработки данных
- Экспертные сервисы в области кибербезопасности
- Защита от целевых и DDoS-атак
- Кибербезопасность критических инфраструктур
- Защита мобильного и онлайн-банкинга

kaspersky.ru/enterprise

© АО «Лаборатория Касперского», 2016. Зарегистрированные товарные знаки
и знаки обслуживания являются собственностью их правообладателей.

ДиалогНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru



Александр БАБКИН
Начальник
Ситуационного центра
информационной
безопасности
Газпромбанка

ТРИ НОУ-ХАУ АЛЕКСАНДРА БАБКИНА

Беседа с создателем и руководителем легендарного SOC Газпромбанка подвела к неожиданному предложению в адрес FinCERT Банка России

Ситуационный центр (СЦ или SOC) Службы информационной безопасности Газпромбанка давно привлекает внимание и вызывает вопросы. С одной стороны, Служба ИБ Газпромбанка регулярно рассказывает о своем детище, внедряя в общественное сознание образ масштабного и зрелого SOC. С другой, закрадываются сомнения: ИТ-инфраструктура Газпромбанка не настолько велика, чтобы поддержать создание и развитие столь крупного Ситуационного центра. В стремлении разрешить эту загадку наш обозреватель Александр БОДРИК встретился с руководителем SOC Газпромбанка Александром БАБКИНЫМ.

ИСТОРИЯ, СТРУКТУРА И ЗАДАЧИ СЦ

— У всякой инициативы есть свое начало. Когда и почему был создан СЦ ГПБ?

— До нашего создания в банке не было ни одной службы ИТ и ИБ мониторинга. И в один прекрасный понедельник в 2010 году, придя на работу, мы обнаружили, что каналы интернета не функционируют ещё с вечера пятницы. Лежит интернет — лежат все — не работают терминалы, банкоматы, то есть все банковские процессы, подразумевающие внешнюю коммуникацию, встали.

Вот для предотвращения подобных инцидентов в рамках служб ИТ и ИБ были созданы дежурная смена и ситуационный центр соответственно. Спроектированная мной тогда архитектура СЦ лежит в его основе и по сей день.

— Минимизация ущерба от масштабных инцидентов требует координации многих подразделений. Как структурирована ваша служба информационной безопасности?

— Расскажу о подразделениях, что прямо задействованы в рамках текущей деятельности

и развития СЦ. Например, проектно-методологический офис выступает агентом изменений ИБ-проектов Банка и представителем безопасности в ИТ-проектах Банка. Управление эксплуатации поддерживает меры, направленные на предотвращение инцидентов (FW, antispan и т.п.), а также выступает в качестве эксперта, когда СЦ расследует технические инциденты. Управление режима обеспечивает user awareness и проводит нетехнические расследования (все инциденты, связанные с людьми, например, нарушения политики ИБ инсайдерами).

— А как структурирован сам СЦ?

— СЦ состоит из двух отделов — отдела администрирования и отдела мониторинга инцидентов. Отдел администрирования предоставляет технический сервис — поддерживает необходимые для работы отдела мониторинга технические средства, по запросу отдела мониторинга инцидентов делает форензик.

Отдел мониторинга инцидентов реализует первую линию по всем инцидентам, а также вторую линию по техническим инцидентам. По нетехническим инцидентам второй линией выступает Управление режима.

— Отличительной чертой крупных инцидентов является пристальное внимание руководства к их разрешению. Кто курирует ситуационный центр в этом плане и службу ИБ в принципе?

— Департамент защиты информации курирует член правления, одновременно курирующий блоки корпоративных клиентов и проблемных активов. Отдельно отмечу, что у служб ИБ и ИТ разные кураторы.

— Насколько я знаю, основной бизнес Газпромбанка корпоративный, а значит, Служба ИБ обладает высоким авторитетом, раз попала в такую компанию. Однако

вы упомянули о мониторинге доступности силами СЦ. Это нетиповая ситуация, почему так?

— Действительно, наш ситуационный центр занимается в том числе и мониторингом доступности банковских ресурсов. Что кардинально отличается от практики, например, телекоммуникационной индустрии.

Производится мониторинг как инфраструктуры ИБ (VPN, FW, IPS), так и ИТ-инфраструктуры, за счет чего СЦ видит полную картину и может разобраться в проблеме даже лучше ИТ, у которых нет доступа к инфраструктуре ИБ. Наверное, можно сказать, что ИБ тут выступает как контроль качества ИТ-сервисов, но, с другой стороны, в ИБ и ИТ Банка инцидент воспринимается по-разному.

Для ИТ инцидент — это когда уже что-то сломалось и нужно срочно чинить (вред Банку уже нанесен). ИБ действует более проактивно, для нее инцидент — это когда произошло событие, которое может повлечь за собой вред для Банка. С точки зрения ИБ проактивная деятельность очень важна для минимизации влияния на бизнес Банка, что также в полной мере соответствует требованиям к управлению инцидентами из СТО БР ИББС.

— Развитые SOC часто идут по пути технического развития, например, форензики, реверс-инжиниринга и киберразведки. Что с этими практиками у вас?

— В 2016 году мы запустили проект по развития функции реверс-инжиниринга. Сейчас покупаем инструменты мирового класса, которые позволяют нам оперативно и качественно снимать все нужные данные.

В части реверс-инжиниринга мы опираемся в первую очередь на нашего антивирусного вендора, а также запустили проект по внедрению «песочницы».

В сфере киберразведки СЦ выступает скорее как потребитель, уже используются бесплатные подписки и идет проработка проектной инициативы по приобретению и использованию платной подписки от одного из российских вендоров киберразведки.

Также в этом году у нас закончены тендерные процедуры и начат проект независимой оценки зрелости СЦ, ведь мы уже 6 лет работаем — пора понять, правильно ли мы работаем с точки зрения передового мирового опыта. Естественно, службы внутреннего контроля и аудита Банка

Производится мониторинг как инфраструктуры ИБ, так и ИТ-инфраструктуры, за счет чего СЦ видит полную картину и может разобраться в проблеме даже лучше ИТ

регулярно помогают СЦ определить зоны потенциальных улучшений, но хотелось бы определить такие зоны именно с точки зрения передового мирового опыта. По итогам оценки сформирован не просто набор отдельных рекомендаций, а фактически целевая операционная модель, включая ИТ-архитектуру, процессную модель, оценку и расчёты достаточной численности штата.

— Мы достаточно углубились в тему, но еще не коснулись индустриальной специфики. Входит ли в СЦ служба фрод-мониторинга?

— В службе фрод-мониторинга как самостоятельном подразделении у нас необходимости нет, так как удалось выстроить высокоэффективный процесс мониторинга фрода в дистанционных каналах обслуживания. Большую часть работы в нем закрывают технологии на базе прообраза искусственного интеллекта (нейронные сети).

По сравнению с основной деятельностью СЦ этот процесс фактически «безлюдный»: операторы выполняют подтверждение подозрительных транзакций (общение с клиентской базой — 30 тысяч ЮЛ), и периодически аналитики СЦ добавляют новые правила выявления фрода. Они у нас в этом плане универсалы: делают правила как для мониторинга ИБ, так и для фрод-мониторинга.

— Многие крупные корпорации при создании SOC выносят операционное ядро в регионы, надеясь снизить затраты и получить доступ к менее конкурентным, чем московский, рынкам труда. Как распределяются по регионам подразделения вашего СЦ?

— Исторически Банк развивался децентрализованно, каждый филиал во многом независим. Поэтому движение в сторону выноса операционных центров в регионы в Банке началось относительно недавно.

Служба ИБ предпочитает концентрировать экспертизу в первую очередь в Москве, так как здесь проще найти высококвалифицированных специалистов, ведь сюда со всей страны стекаются лучшие кадры.

ТЕХНОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СЦ

— Газпромбанк известен на рынке высокой степенью автоматизации SOC. Какие ключевые системы Вы бы выделили?

У нас и правда практически полный комплект систем — C MDB, сбор с наших и ИТ-источников, нормализация, агрегация и корреляция в события с признаками инцидентов (посредством SIEM от одного из лидеров рынка), обработка инцидентов в сервис-деске службы ИБ, Security BI («светофоры для менеджмента») — всю архитектуру возможно увидеть на Рисунке 1.

— Остановимся на C MDB. Главной проблемой таких систем обычно является их постоянно устаревающее наполнение.

Мы практикуем конфедеративный подход к C MDB. Вручную ведем свою инфраструктуру, интегрируемся с развивающимся C MDB-проектом ИТ. Если в ходе обработки инцидента мы обнаруживаем «темные пятна» (например, инцидент, что не привязан ни к одному элементу нашей сервисно-ресурсной модели) или неактуальную информацию, мы стараемся устранить этот недостаток в своей C MDB.

Актуальная C MDB критически необходима для здравой оценки влияния инцидента на бизнес. В планах есть и развитие систем класса Asset Discovery, но это не самая приоритетная инициатива нашего портфеля проектов развития ИБ.

— Обсудим Ваш Service Desk. Он общий с ИТ или свой?

— У нас свой, т.к. у инцидентов поля прописаны в четком соответствии с классификатором

инцидентов по требованию ЦБ, а у ИТ-шников все по-другому.

К счастью, у нас есть возможность иметь свою инфраструктуру автоматизации СЦ.

— Да, для служб ИБ, что сидят вместе с ИТ в одном SD, характерна проблема приоритетности задач по доработке SD для ИТ над задачами ИБ. Как Вы решаете проблему контроля регионов, учитывая слабые каналы связи в традиционных нефтегазовых провинциях?

— Мы ставим в регионах «экспресс» редакцию нашего SIEM, и пересылаем в центр не сырые, а отфильтрованные данные.

ПРОЦЕССЫ РАБОТЫ СЦ

— Как распределяются полномочия в СЦ в рамках мониторинга угроз?

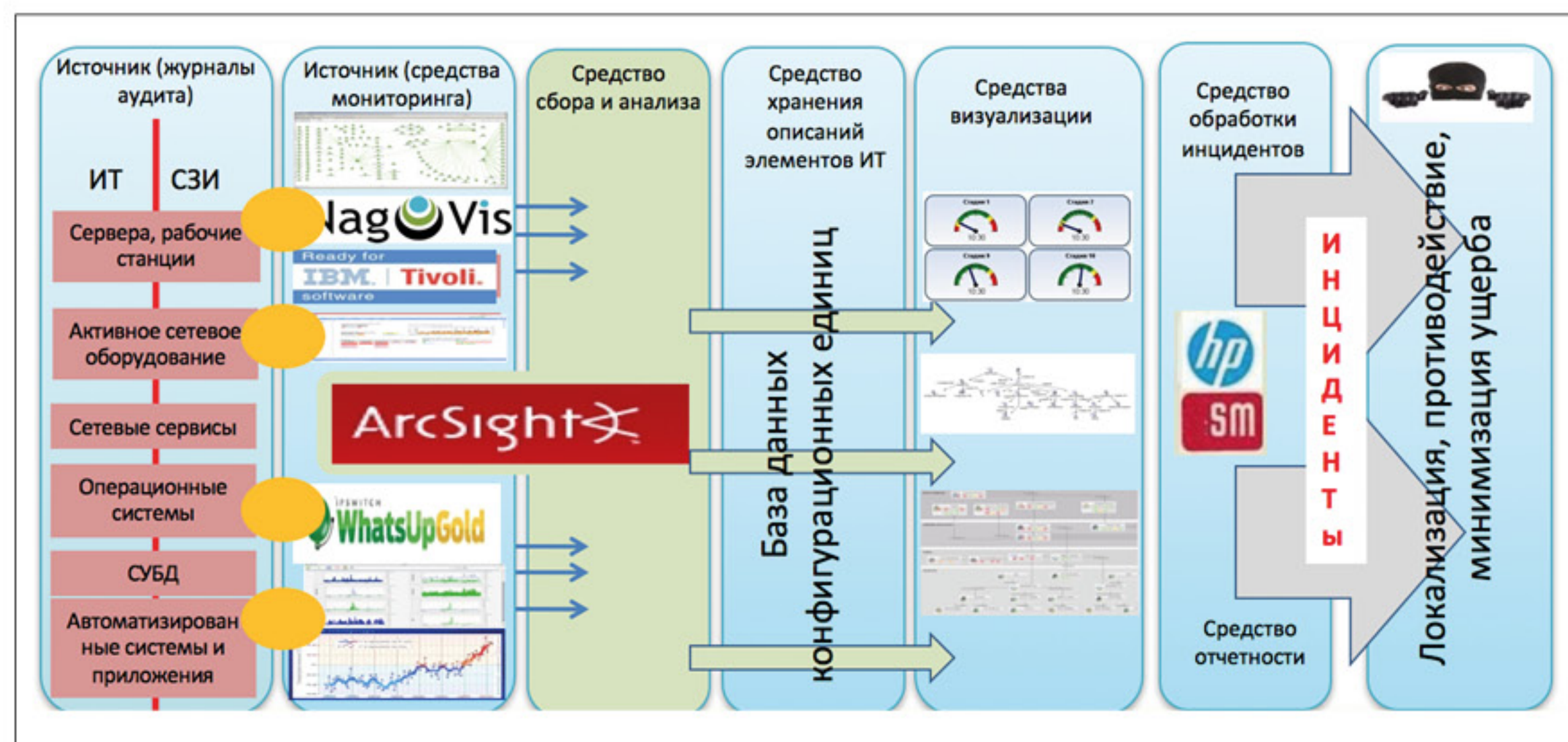
— В СЦ существует четыре роли в рамках процесса реагирования и расследований инцидентов — оператор, аналитик, расследователь и администратор.

Оператор производит мониторинг введенных в работу кейсов, подтверждает и классифицирует инцидент, расследует инцидент -реагирует согласно инструкциям (выступает в роли расследователя), либо эскалирует руководителю SOC (мне).

Дежурный и производит подключение систем к ситуационному центру, уже выступая в роли администратора.

Этот же дежурный выступает в роли аналитика — составляет правила для детектирования угроз. В итоге центр иногда выступает агентом

Рисунок 1.
Структура построения SOC



изменений, так сказать, «передовиком производства», везде говоря «А еще вот это надо улучшить».

Например, пошли АPT-атаки. Мы стали получать о них информацию из различных источников — от коллег по межбанку, из рассылки FinCERT, и поняли, что, во-первых, типовое начало такой атаки — это электронное письмо, во-вторых, на рынке существуют решения по анализу таких писем и их вложений («песочницы»). На данный момент проект по «песочнице» уже в активной фазе — внедряем.

Таким образом, у нас не существует типовой многоуровневой модели SOC («пирамида»), у нас скорее «кольцо».

— То есть у Вас выработана своя ролевая модель работы?

— Это действительно модель, причем, мы стараемся придерживаться этой модели уже шесть лет. И пока никто меня не смог разубедить в ее неправильности. Мы не всегда успеваем ее актуализировать, потому что я по каждому правилу требую паспорт, например. В паспорте должно быть прописано: автор, логика этого технического правила, меры реагирования, меры оповещения руководства.

— Да, у Вас очень высокий уровень формализации процессов.

— Когда в SIEM валится 4000 событий в секунду, возникает вопрос: как аналитику начать с этими событиями работать. И тут я выделяю два подхода.

Подход «снизу-вверх», как у трейдеров — технический анализ. Раз у нас много данных, их возможно визуализировать на графиках. Раз есть графики, то у любого из них есть baselines — нормальные и аномальные состояния.

Например, все сотрудники используют систему X с 10 до 18 часов, а некий сотрудник с 8 до 9. Или мы видим, что типового спада объема интернет-трафика по окончании рабочего дня не происходит. В таких случаях регистрируются события с признаками инцидента, и оператор производит проверку.

Однако, чтобы первоначально выявить такое нетипичное поведение, дежурному надо собрать данные, построить графики, посчитать отклонения и т.д. Тут нужен очень серьезный мат. аппарат.

Исходя из внутренней нормативной базы (политики безопасности, модель угроз), организация планирует обеспечивать конфиденциаль-

ность информации. Какие могут быть угрозы конфиденциальности? Например, нарушение конфиденциальности учетной записи. Банальный брутфорс.

Проводим самопроверку — нормативные основания есть, угроза такая есть, есть ли в подлежащих мониторингу системах данные об успешных и неуспешных попытках входа? Есть, — можем описывать и запускать в работу.

— Сейчас на Западе очень популярна тема обмена информацией (data sharing). Обмениваетесь ли Вы с кем-то?

— У нас налажено хорошее рабочее взаимодействие с FinCERT. Я считаю создание такой структуры очень правильным шагом, и она уже принесла много пользы банковскому сектору.

ТРИ НОУ-ХАУ СЦ ГАЗПРОМБАНКА

— Мы обсудили много технических моментов, давайте поговорим о кадрах. Где СЦ берет людей, как развивает, мотивирует и удерживает?

— Когда мы набирали людей, было поставлено принципиальное условие — исключительно с высшим образованием в сфере защиты информации. Мы не переучиваем людей с хелпдеск, мы сразу берем профессионалов в сфере безопасности.

В части обучения. Банк регулярно выделяет средства на обучение в России и мире. Зарубежное обучение производится в том случае, если нужных курсов в России нет, а так часто бывает по тематике SOC.

Естественно, инвестиции в обучение плюс разнообразная работа (совмещение ролей) повышают стоимость наших сотрудников. Банк это понимает, и реализует целую программу мероприятий для мотивации специалистов. Во-первых, денежная мотивация — индексация, увеличение по мере повышения производительности, дополнительная оплата ночных дежурств (как велит ТК), дополнительная оплата в случае двух смен за 4 дня (по умолчанию график сутки / трое, но молодые специалисты готовы работать и через сутки).

Когда в SIEM валится 4000 событий в секунду, возникает вопрос: как аналитику начать с этими событиями работать

Рисунок 2.
Сбор информации
об объектах мониторинга

уровень корреляции	состав корреляции	тип сформированной корреляции							пункты в таблице корреляций	кол-во правил корреляции	кол-во технологических правил	кол-во правил выявления инцидентов ИБ ДЦ/К
		ТОС7	ТОС6	ТОС5	ТОС4	ТОС3	ТОС2	ТОС1				
	общее ТОС4								4	5.		
Правила уровня ТОС4 (Операционные Системы)	ТОС3								3	5.1		
									2	5.1.1		
									1	5.1.1.1		
								1	5.1.2			
	ТОС2								2	5.2		
	ТОС1								1	5.2.1		
									1	5.3		
Правила уровня ТОС3 (Сетевые сервисы)	общее ТОС3								3	6.		
	ТОС2								2	6.1		
									1	6.1.1		
	ТОС1								1	6.2		
Правила уровня ТОС2 (сетевые устройства)	общее ТОС2								2	7.		
	ТОС1								1	7.1		
Правила уровня ТОС1 (физическое устройства)	общее ТОС1								1	8.		

Во-вторых, мотивация гибким графиком работы. Специалист имеет много свободного времени и может себе позволить то, что не могут люди с 8х5.

В-третьих, мотивация разнообразием работы, в частности, нашим распределением ролей. Если человек сидит в смене, т.е. на сутки, то мы стараемся подключить его на первую линию (разбор инцидентов). Если же он, предположим, сегодня отоспался, ушел в 8 часов утра, завтра выходит в день (только в день). Завтра он станет аналитиком, будет делать правила и анализировать повторяющиеся инциденты.

— Значит, у вас больше человекочасов, чем должно быть при стандартном расписании? То есть человек работает больше 40 часов в неделю? Это фактически некое ноу-хау по повышению отдачи от людей!

— Специалисты молодые — глаза горят, поэтому они говорят: хочу, хочу. А — им это интересно, Б — банк за это ещё и деньги платит. Почему бы не выйти, не повысить свою компетенцию, да еще и деньги получить.

Но если уж говорить о ноу-хау, то это в первую очередь — ТОСы.

— А что такое ТОСы?

— В свое время мы увязали понятия СТО БР ИББС с той визуализацией, которая у нас есть. В стандарте Банка России сказано, что кредитная организация и служба информационной безопасности обязана обеспечивать информационную безопасность на каждом уровне. Вот эти ТОСы — их ровно 7. Они очень сильно по-

вторяют семиуровневую модель OSI. Один в один, практически. Форму возможно увидеть на Рисунке 2.

— То есть это некий security framework?

— В целом да, мы используем модель ТОСов для планирования и разработки правил детектирования инцидентов. Фактически это таблица, как мы ее называем, Менделеева по ИБ. Как и в таблице Менделеева — здесь пока много незакрытых элементов.

Например, когда аналитик создает правило детектирования (той же DDOS атаки), он должен это правило вписать в определенную клеточку. Ее местоположение зависит от того, какого свойства информация была нарушена и какого уровня объект «защищает» это правило.

У каждого уровня ТОСа есть направление защиты: конфиденциальности, целостности и доступности. Когда мы говорим об инциденте, связанном с DDOS атакой, это означает нарушение доступности сетевых сервисов. То есть второй-третий уровень. Это точно не физический уровень и точно не шестой-седьмой...

Это конкретно сбой на сетевом уровне, причем, направленный на нарушение доступности, а не конфиденциальности или целостности. И получается матрица: по вертикали — ТОСы, по горизонтали — КЦД (конфиденциальность, целостность, доступность). Когда создается правило, то на пересечении определенного уровня и определенного столбца вписывается цифра: сколько правил для этого создано.

Большинство полей пустые. Почему пустые? Потому что это задача на «подумать», какие должны быть правила, чтобы выявлять угрозу целостности, конфиденциальности, доступности на том или ином ключе.

ТОСы мы используем даже при общении с руководством. В частности, представляя результаты работы куратору.

Мы столкнулись с тем, что создать правило, которое выявляло бы инциденты с нарушением целостности (столбец целостность) — это самое сложное. Очень многие вещи нельзя выявить только из-за того, что системы (контролируемые системы) не обладают достаточно детальным журналированием (*legacy, давняя проблема ИБ во многих отраслях — прим. автора*).

— Да, действительно, ноу-хау как минимум в России, чем-то похоже на американский фрейм-ворк VERIS. И напоследок, что бы вы выделили среди направлений развития СЦ?

— Сейчас мы прорабатываем возможность мониторинга доступности и эффективности бизнес-процессов.

Согласно требованиям ЦБ служба ИБ должна обеспечить безопасность банковских технологических процессов. Некий абстракт. Когда мы говорим про банковские технологические процессы — это практически формализованный технологический процесс. Входные данные, выходные, функции преобразования...

Второй момент. На дворе 21 век, любые технологические процессы оцифрованы.

Таким образом, у нас есть возможность деконструировать бизнес-процесс на элементы (с помощью сервисно-ресурсной модели) — сер-

вер приложений, СУБД, ОС, инфраструктура... и используя матмодель (например, затухающего коэффициента), вывести для бизнеса монитор (независимый от ИТ).

Если представитель ИТ по телефону сообщит «все ОК» — по монитору можно будет понять, так ли это.

Например, сервис SWIFT. Сервис основан на 4 серверах (кластер) — 2 СУБД и 2 appservers. Но, если сервис функционирует как задумано, то бизнесу не важно, сколько серверов.

Мы попытались в процесс мониторинга доступности сервисов вовлечь бизнес и объяснить, что бизнес сможет понимать, правильно ли все функционирует, смотря на всего лишь один понятный индикатор. Неважно, что за этим индикатором стоит большая сервисно-ресурсная модель, это уже наши проблемы.

Теперь бизнес-языком можно с ними общаться: «Ребята, у вас система простаивает, или наоборот?» У нас была ситуация, когда все системы штатно работают, а сам процесс начинает тормозить (KPI не выполняются). Что ж такое? ИТ-шники работают, все корректно, а тормозит где-то, как они называют, ванночки. Ванночки не переливаются.

Выясняется, в определенный момент, определенный отдел слег с гриппом — больше половины сотрудников на больничном. У них нагрузка и разошлась. Все системы работают, но «переливание ванночек» стало подтормаживать.

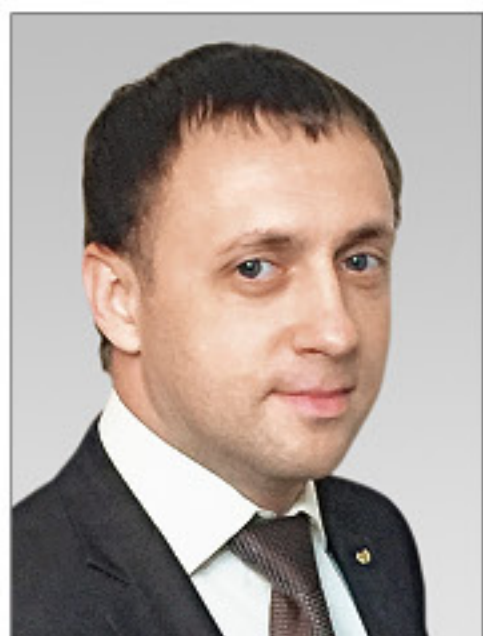
А вот в случае выхода из строя одного из серверов в кластере бизнесу, наоборот, такой инцидент может быть неинтересен — сервис-то работает исправно.

ОТ РЕДАКЦИИ

Очевидно, что Ситуационный центр Газпромбанка — один из наиболее развитых СЦ в стране, и благодаря ряду ноу-хау (достойных быть внесенными в своды лучших практик) ухитряется закрывать относительно небольшими силами многотриллионные активы банка ТОП-5 страны. Но в то же время существуют десятки и сотни банков, которые не могут себе позволить даже бледного подобия практик Газпромбанка. Может быть, Банку России стоит развивать FinCERT не только в сторону координации управления инцидентами, киберразведки и других привычных аспектов модели CERT. Например, продумать модель Community SOC, когда Банк России или уполномоченный им банк станет центром экспертизы по мониторингу кибератак, и все, кто захочет подключиться, например, к БЭСП, будут обязаны заказать такой сервис для всей своей сети или ее сегмента.

Ровно по такой модели сегодня работают крупнейшие глобальные корпорации, к централизованным информационным системам которых не получить доступ, если не соответствовать внутренним ИБ-стандартам, не заказывать внутренний сервис SOC.

ЭФФЕКТИВНАЯ DLP В ЭПОХУ ПЕРЕМЕН



Сергей ЗИНОВКИН
главный инженер отдела
обеспечения процессов
SOC Сбербанка



Игорь АГУРЬЯНОВ
ведущий инженер отдела
обеспечения процессов
SOC Сбербанка

Постоянные изменения — единственный путь к эффективной DLP-системе

«**Ч**тоб вам жить в эпоху перемен!» — проклинали древние китайцы своих недругов. Не потому, что перемены — это обязательно плохо, а потому, что успех в такую «интересную эпоху» требует колоссальных усилий по изменению самого себя.

Мы это прочувствовали. Гаджеты, выпущенные пару лет назад, теряют половину своей стоимости, ибо «древняя модель». Как-будто из ниоткуда появились новые компании, захватив «голубые океаны» и став транснациональными корпорациями. Постоянно приходится повышать свою квалификацию, чтобы оставаться в тренде. Чтобы преуспевать, приходится меняться.

В изменчивом мире мы защищаем то, что представляет «коммерческую ценность в силу неизвестности третьим лицам» и интересы клиентов и партнёров. В этом нам должны помочь системы предотвращения утечек информации (DLP — Data Leak Prevention). DLP-система — инструмент, который не работает «из коробки» и требует длительной «тонкой» настройки:

- ♦ мы должны знать, что именно защищать при помощи DLP-системы (сформировать перечень конфиденциальной информации);
- ♦ научить систему различать конфиденциальную информацию в потоке трафика;
- ♦ научить систему отличать, когда конфиденциальная информация отправляется «вовне» легитимно.

Причём эта настройка в успешной организации на самом деле не длительная, а непрерывная, в силу постоянных изменений, о которых мы говорили выше. В крупных компаниях (десятки тысяч работников) изменений столь много, что настройка за ними не успевает. Она не

тривиальна, требует проб и ошибок. Отсюда — ИТ-риски установки DLP-системы «в разрыв» (в режим блокировки), которые риски возникают на этапе настройки системы (а она идёт постоянно). Но даже при корректной и точной настройке правила с первого раза (чтобы система не срабатывала ошибочно, блокируя безобидные письма) есть вероятность, что система не справится с множеством правил в политике, помноженным на огромный объём трафика, и «упадёт».

Кроме того, т.к. настройка не успевает за изменениями, мы рискуем пропустить утечку конфиденциальной информации — нужное правило не было настроено в момент утечки. Поэтому важно хранить архив перехваченной информации, что позволит проводить её ретроспективный анализ. Это противоречит концепции «западных» DLP, когда хранится только та информация, на которую DLP-система сработала.

Еще одна головная боль, вызываемая переменами — новые технологии передачи данных. Проблема, над которой постоянно работают вендоры DLP-систем. Нет гарантий, что Google завтра не изменит протокол загрузки данных в свое облако на более безопасный, и не распознаваемый DLP-системой, что Microsoft не внедрит в Skype дополнительную фичу и при звонке не будет модулировать голос собеседников, чтобы стенографически передавать дополнительную информацию... В борьбе за клиента ИТ-компании тоже меняются и меняют свои продукты, а DLP-вендоры за ними не всегда успевают.

Если вам доведётся работать с DLP-системой в большой и динамичной компании, то резонными будут вопросы, как все изменения отслеживать? Как получать информацию от сотен тысяч человек, инициирующих, прорабатывающих, апробирующих изменения?

КАК ВООБЩЕ НАЧАТЬ НАСТРОЙКУ DLP-СИСТЕМЫ?

Ниже приведены подходы, которые позволят произвести базовую настройку DLP-системы без взаимодействия с другими структурными подразделениями, отслеживать изменения и адаптировать под них DLP. Прежде чем приступать к использованию этих подходов, мы рекомендуем отключить преднастроенные правила реагирования, которые установил производитель — они будут нам мешать, а также не использовать режим блокировки до тех пор, пока правила не будут отточены (с учётом нагрузки), а бизнес не примет риски установки «в разрыв».

Несмотря на непрерывность изменений, некоторые вещи меняются медленно. Один из жёстких признаков конфиденциальности документа, которому уже не один десяток лет, — его гриф. Реагирование на определённый гриф («Для служебного пользования», «Коммерческая тайна»...) — самый простой по настройке механизм выявления утечек (метод «стоп-слов»). Если такой документ однажды попадёт к нам в систему, мы поймём его по грифу. Мы скоро увидим, что по этим «стоп-словам» ловится много того, что ловить бы не хотелось: дисклеймеры в подписях контрагентов в переписке, драфты договоров (в которые включён пункт о конфиденциальности с указанием грифов), художественная литература... Но среди всего этого многообразия, если у нас в организации документы грифуются, обнаружатся и настоящие утечки.

Такой инцидент даст нам новый материал для настройки DLP-системы. У нас появится документ, на основании которого мы сможем ловить «похожие» и уже даже без грифа (на случай, если пользователь забудет его проставить или нарушитель не забудет удалить). Детектирование в трафике «похожих» документов называется *технологией цифровых отпечатков*. Ловить точно такие же документы — редкая задача, поэтому настраивается степень «похожести». Работает это примерно так:



DLP-система — инструмент, который не работает «из коробки» и требует длительной «тонкой» настройки

- ♦ защищаемый документ (файл) разбивается на блоки, с каждого из которых снимается хэш (конкретные алгоритмы различаются, некоторые даже запатентованы);
- ♦ файлы в трафике хэшируются по тому же алгоритму;
- ♦ при совпадении определённого числа хэшей с хэшами защищаемого документа происходит срабатывание.

В один или несколько блоков может попасть не интересная с точки зрения защиты информация, что приведёт к ложным срабатываниям (чем ниже порог «похожести», тем больше). В то же время высокий порог «похожести» приведёт к тому, что мы не сможем обнаружить незначительное изменение части документа, которая имеет ценность.

Эти «жёсткие правила» («стоп-слова» и цифровые отпечатки) просты в настройке, но их легко обойти. И в условиях постоянных изменений они быстро теряют свою актуальность. Тем не менее, они позволяют нам получать заказы от бизнеса (каждый работник становится нашим потенциальным заказчиком: заказ он оформляет в виде надписи на документе, сигнализируя нам (и DLP-системе), что информация в нём требует защиты). Благодаря таким



заказам постепенно у нас соберётся репозиторий конфиденциальных документов, и их нужно будет классифицировать. В основу классификации рекомендуем заложить «Перечень конфиденциальной информации» — к какому пункту «Перечня...» относится этот документ.

«ПЕРЕЧЕНЬ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ» — ВАЖНОЕ УСЛОВИЕ ЭФФЕКТИВНОЙ РАБОТЫ DLP

Скорее всего, в этом перечне будут указания на некоторые формы документов. В «Перечне конфиденциальной информации», который даёт Центробанк в своих рекомендациях¹, например, содержатся такие пункты:

- ♦ организационно-распорядительные акты (приказы, распоряжения) организации БС РФ;
- ♦ информация об организационно-штатной структуре и её изменениях.

Заметим, что во многих приказах встречаются слова (фразы): «приказ», «приказываю», «в целях», «контроль за исполнением», «утвердить», «обеспечить», «выполнить» и т.д. А для «информа-

ции об организационно-штатной структуре...» характерны слова (фразы): «должность (специальность, профессия), разряд, класс», «штат в количестве», «тарифная ставка (оклад)», «надбавки, руб.» и т.п. Поиск по этим словам и фразам позволит пополнить нам примеры документов, подпадающие под те или иные пункты перечня. Возможно, сразу обнаружить утечки.

В дальнейшем на основании множества документов, подпадающих под один и тот же пункт «Перечня конфиденциальной информации», мы сформируем при помощи «весов» более мягкие и точные правила, которые позволят автоматически определять, что документ относится к тому или иному пункту перечня (*технология лингвистического анализа*).

Суть технологии лингвистического анализа сводится к назначению ключевым словам и фразам определенного «веса». Когда сумма «весов» в документе переваливает через некий порог либо соотношение частоты встречаемости этих ключевых слов близко к соотношению их «весов», происходит срабатывание. Эта техноло-

¹ РС БР ИББС-2.9-2016 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации

гия довольно точно детектирует пункт перечня, к которому документ относится, несмотря на то, что форма документа уже значительно поменялась (по сравнению с теми, на основании которых мы сделали эту политику).

Но есть и такие документы, информация в которых изменяется практически полностью. Или неизменяемые слова и фразы документа употребляются повсеместно. Например, таблица с именами клиентов, их контактной информацией и, скажем, суммой депозита. Такие базы зачастую ведут «на коленке» менеджеры или выгружают из корпоративной CRM.

Во многих организациях это наиболее чувствительный к утечке актив. Для обнаружения таких утечек стоит поискать для начала в исходящем трафике таблицы (.xls, .xlsx, .csv) — наиболее вероятный формат хранения выгрузок клиентских баз.

Кроме того, некоторые DLP-системы способны обнаружить в трафике документы, в которых много раз повторяется одно и то же слово. Если это слово «ООО», «ПАО» или «АО», то очень вероятно, что мы имеем дело с какой-то базой юридических лиц. По сути, ту же функцию выполняет *технология поиска шаблонов* текстовых объектов: она позволяет находить строки символов, построенные по определённому алгоритму (например, номера банковских карт или ИНН).

Ряд DLP-систем позволяет провернуть ещё одну хитрость: детектировать объекты, в которых встречается более X записей из списка. Скачав в сети Интернет список самых популярных русских фамилий (например, 1000 фамилий) и установив X, равным, например, 50, мы получим правило, которое детектирует объекты, в которых содержится более 50 популярных русских фамилий. Такой объект с большой долей вероятности — база физических лиц или индивидуальных предпринимателей.

Обнаружив такие таблицы, мы можем использовать названия некоторых столбцов, назначая им определенный «вес» для дальнейшего детектирования аналогичных таблиц и сопоставляя с пунктами «Перечня информации ограниченного доступа».

Благодаря этим подходам мы выявим ряд утечек даже во время пилотирования DLP-решения. Но главное, они позволяют постоянно формировать и дополнять базу правил, которая будет соотноситься с «Перечнем конфиденци-

Также необходимо будет много работать с тем, что какая-то информация, хоть и защищаемая, всё же куда-то и кем-то может отправляться

альной информации». А значит, меняться вместе с миром и достигать успеха.

НО НА ЭТОМ МЫ НЕ ОСТАНОВИМСЯ...

Следует помнить, что эти подходы не единственные: их также необходимо развивать и придумывать новые «хитрости», а некоторые правила, которые раньше работали, придётся изменять или удалять из-за частых ложных срабатываний.

Мы даже обнаружим ряд правил, которые срабатывают практически безошибочно и редко меняются: при условии согласования рисков на основании таких правил мы сможем даже блокировать утечку. Согласитесь, отчёт «мы заблокировали попытку утечки» выглядит куда лучше, чем — «мы нашли утечку». Но отслеживать изменения и корректировать настройки придётся ещё тщательнее.

Также необходимо будет много работать с тем, что какая-то информация, хоть и защищаемая, всё же куда-то и кем-то может отправляться. Иногда будет достаточно настроить исключения из правил, но часто эти «кем-то» и «куда-то» — ситуационные (например, острая необходимость поработать с конфиденциальной информацией на дому). И тогда мы уже будем прорабатывать возможные ситуации, процедуры согласования отправок и «разбора полётов» для таких ситуаций, дополнительные процедуры контроля... Впрочем, процедуру «разбора полётов» придётся проработать для всех ситуаций. А ещё процедуру ознакомления и обучения работников — что можно и что нельзя отправлять.

* * *

И процедуры эти тоже будут постоянно меняться. В том числе нами. Но постоянные изменения — это единственный, пусть и сложный, путь к эффективной DLP-системе. Чтобы достигать высоких результатов, требуется много усилий — и так и должно быть. Удачной «эпохи перемен», коллеги!



Андрей ЯНКИН
руководитель отдела
консалтинга Центра
информационной
безопасности компании
«Инфосистемы Джет»

SOC 2.0.

АППЕТИТ ПРИХОДИТ ВО ВРЕМЯ ЕДЫ

Но пока уровень зрелости базовых процессов российских SOC по пятибалльной шкале находится в районе единицы

Пока ИБ-сообщество продолжает споры о том, что такое SOC, компании и государственные учреждения вовсю ведут стройку и эксплуатируют эти центры. То, что получается на практике, удивительно редко соответствует каноничному представлению о SOC. Кто-то не может сдвинуться с точки SOC v0.1, но если уж взялся строить, то и на версии 1.0 остановиться сложно. Хочется больше функций, больше возможностей. Рассмотрим, какие метаморфозы претерпевает SOC в российских реалиях, и какие подводные камни встречаются на пути к SOC 2.0.

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

Самый популярный кейс, с которого зачастую начинается интеграция SOC в физическую и инженерно-техническую безопасность, — это учет прохода сотрудников через турникеты, чтобы отслеживать логины на АРМ пользователей, физически отсутствующих в здании. Для любой популярной SIEM-системы не сложно сделать коннектор для СКУД и создать соответствующее правило. Но многие хотят двинуться дальше и делают на базе SOC центр мониторинга инженерно-технической защиты. SIEM создаст информационную шину, которая опутывает все подразделения компании и позволяет вывести сигналы от систем защиты в единый центр. Но тут же возникают и проблемы. В мире физической безопасности существует еще больший зоопарк средств защиты, чем в ИБ. В одной компании может использоваться по десятку моделей СКУД, сигнализаций, противопожарных систем. Создавать и поддерживать такое число нестандартных коннекторов для SIEM очень не-

удобно. Кроме того, системы генерируют огромные объемы информации, пожирающие каналы связи и недешёвые лицензии на EPS в SIEM. А с частью информации (например, видео) SIEM вообще работать не умеют. Тут на помощь приходят системы класса PSIM (physical security information management). У них есть коннекторы к сотням моделей устройств физической безопасности, несложная, по меркам SIEM, система правил позволяет пересылать только важную информацию, а видеоданные можно передавать как ссылку на интерфейс PSIM. Или вообще выстроить на PSIM альтернативную сеть сбора данных и коррелировать информацию с SIEM уже в центре (вариант для не самых больших компаний). Сама необходимость корреляции именно сырых событий между ИТ и системами физической безопасности должна быть здраво оценена перед строительством системы. Практика показывает, что она нужна не так уж и часто. Проблема возникает также с тем, что у инцидентов ИБ и инцидентов физической и инженерно-технической безопасности разные алгоритмы обработки, свойства, классификация и т.п. Да и просто в компаниях ими обычно занимаются совершенно разные люди, свести которых под крышей одного центра реагирования бывает совсем непросто.

БОРЬБА С МОШЕННИЧЕСТВОМ

Данные, собираемые SOC, могут использоваться, в том числе и для анализа поведения пользователей и обнаружения фактов мошенничества (например, воровство базы клиентов). А отдельные системы борьбы с мошенничеством не уступают по сложности корреляционных и об-

наруживающих механизмов SIEM и IPS. Например, в случае контроля фрода в каналах ДБО и кросс-канальных схем мошенничества в банковской сфере. Направления ИБ и антифрода взаимно дополняют друг друга, но в большем выигрыше определенно антифрод, потому что поле его анализа существенно расширяется за счет традиционных источников данных SIEM-систем. Физическое совмещение дежурных смен по направлениям натывается на проблемы ограничения доступа и разделения обязанностей (SoD). Корпоративные политики могут сделать это и вовсе невозможным. Различаются и процессы обработки инцидентов. На уровне техники проблем меньше и в базовом варианте антифрод может использовать ИБ-системы SOC просто как ценный источник информации для обнаружения и расследования мошеннических действий, ничего не предоставляя SOC.

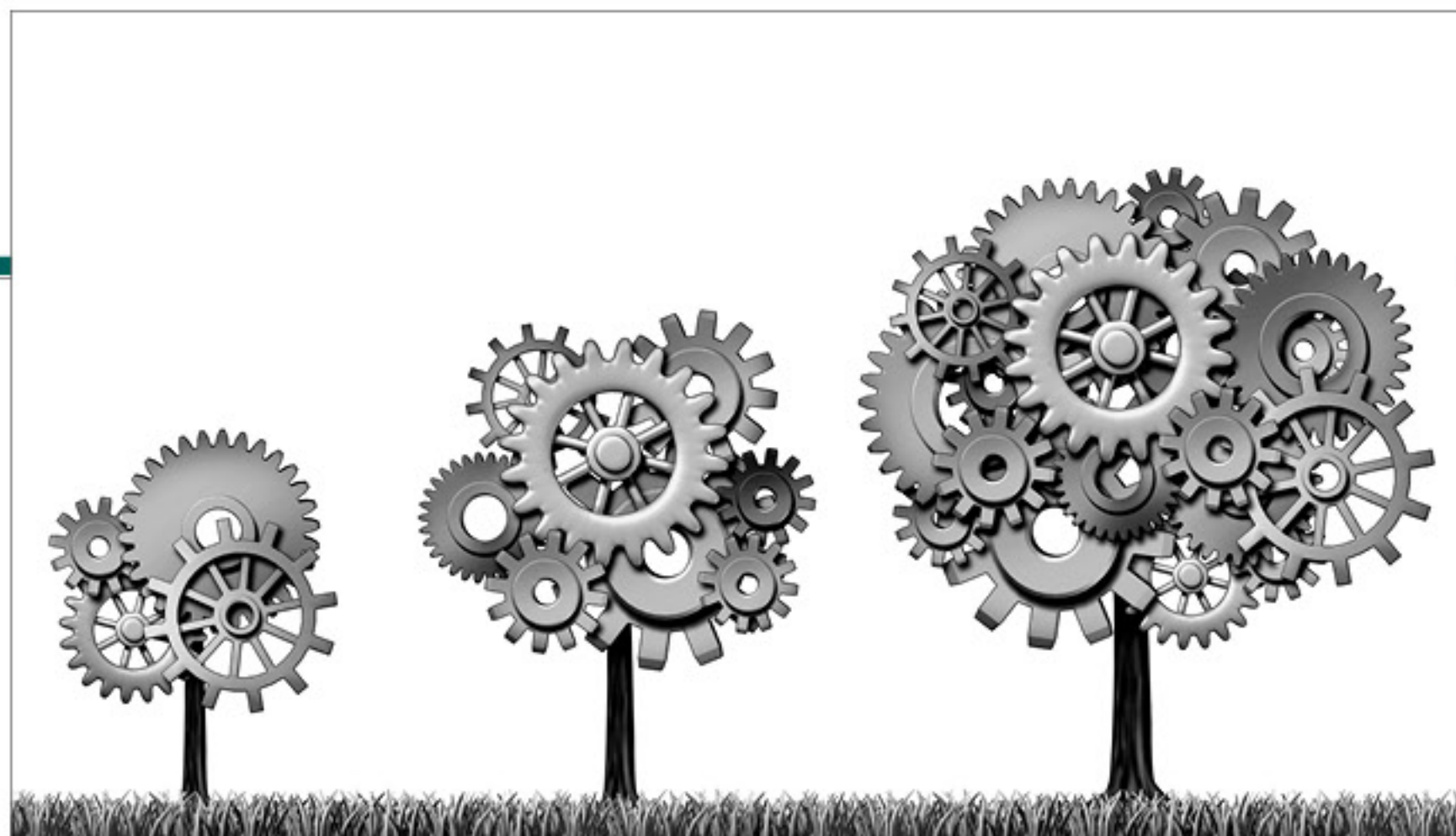
СТРАТЕГИЧЕСКИЙ УРОВЕНЬ

В рамках работы с инцидентами ИБ накапливается ценная статистика по реальным угрозам, идет анализ внешних источников, оценивается эффективность защитных мер. Логично использовать эти данные при планировании развития ИБ в компании. Но необходимо понимать, что это дополнительное преимущество, а не основная задача.

SOC — мощный инструмент и большая стройка. Его заказчиком в компании обычно является кто-то из крупных руководителей. Он формирует основные требования к системе. Сам термин SOC говорит о том, что он должен создаваться в первую очередь для решения оперативных задач по управлению инцидентами. Однако, обсуждать блок-схемы обработки событий безопасности скучно, поэтому руководство переключается на более глобальные задачи. Например, «SOC должен в автоматическом режиме анализировать геополитическую обстановку в мире и прогнозировать будущие угрозы ИБ». Задача строителей SOC состоит в том, чтобы не только «приземлить» эти требования до чего-то реализуемого и реально полезного, но и выстроить основу SOC, сконцентрированную на рутинной обработке инцидентов. Иначе этот голем на глиняных ногах рухнет под своим весом, так и не сделав первого шага.

ЭКСПЛУАТАЦИЯ СРЕДСТВ ЗАЩИТЫ

Может показаться, что смешение инцидент-менеджмента и администрирования СЗИ — это вынужденная мера небольших организаций



Если уж взялся строить SOC, то на версии 1.0 остановиться сложно. Хочется больше функций, больше возможностей

с ограниченным штатом. О SOC здесь, понятно, речи не идет. На деле даже в крупных организациях эти функции часто смешивают. Где-то это политическое решение, где-то реальное непонимание недостатков такого подхода. В любом случае, нарушение разграничения полномочий, отвлечение сотрудников 1-й и 2-й линии SOC от основных обязанностей, конфликт интересов на уровне руководства SOC — неадекватная плата за плюсы такой интеграции. Если сдвинуть ситуацию невозможно (например, не удастся пересмотреть организационно-штатную структуру), приходится строить искусственные «стены» внутри SOC, разделяя обязанности. Половина SOC — это настоящий SOC, а вторая половина только так называется.

SOC должен иметь стратегический план развития. Выход за пределы классических ограничений — хорошая его часть. Как и для человека, так и для SOC, чтобы достичь больших целей, надо их сформулировать и планомерно к ним двигаться. Однако, многие российские SOC имеют уровень зрелости базовых процессов управления ИБ в районе единицы по классической пятибалльной шкале модели зрелости (Capability Maturity Model, CMM). Думаю, сначала надо сконцентрировать большую часть ресурсов на этой проблеме. На прочном фундаменте базовых процессов и технологий можно построить систему, способную на гораздо большее, чем рутинная обработка типовых инцидентов, построить тот самый SOC 2.0.



Алексей МАЛЬНЕВ
заместитель директора
департамента ИБ
АМТ-ГРУП

ПОДБИРАЯ ЛУЧШЕЕ ДЛЯ SOC

Как фильтровать маркетинговые тренды

За последние 10 лет в области информационной безопасности объявлялось множество «революций», которые на поверку оказывались лишь маркетинговым ходом. Цель такого хода — дать новый импульс продажам, представив эволюционное развитие отдельного продукта как некую революцию и абсолютно новый подход. Проблема в том, что часто конечный потребитель не в состоянии определить, появился ли на рынке новый продукт, полезный для бизнеса, или что-то давно известное «обернули в новую упаковку». Как правило, планируя SOC, у нас в запасе есть только «один выстрел», чтобы реализовать с первого раза максимально эффективную службу с оптимальным набором технических инструментов. Поэтому мы должны правильно фильтровать маркетинговые тренды.

Например, развитие межсетевых экранов шло по пути (упрощенно): Stateless (packet) Firewall → Statefull Firewall → UTM firewall → Application Firewall → Next Generation Firewall. На мой взгляд, это показательный пример эволюционного развития одного класса решений ИБ. Нужно ли менять удовлетворительно работающий UTM на NGFW? Далеко не всегда. Являются ли новые функции NGFW необходимыми? Как правило, они полезны, но не необходимы даже с поправкой на особую модель угроз: IPS и потоковый антивирус в составе UTM тоже делает инспекцию приложений, пусть и без набора функций NGFW.

Часто конечный потребитель не в состоянии определить, появился ли на рынке новый продукт, полезный для бизнеса, или что-то давно известное «обернули в новую упаковку»

Также давайте вспомним про внезапный рост популярности такого явления, как АРТ (Advanced Persistent Threat) и развития «специализированных» решений борьбы с АРТ. А раньше АРТ не было? Угрозы, конечно, каждый год растут, но это касается любого типа угроз. И разве бывают IPS, не противодействующие АРТ — таргетированным и сложным атакам? Так или иначе любое средство ИБ в какой-то степени разработано для борьбы с АРТ. Глобальная задача любого решения ИБ одна: обнаруживать и подавлять злонамеренную активность, как обособленную, так и в составе сложной АРТ-атаки. Поэтому менять корректно настроенный и обновляющийся (сигнатурные базы) сигнатурный IPS на сигнатурный АРТ IPS в большинстве случаев не представляется необходимым.

Это не камень в огород маркетинга — это жизнь и, вообще, нужно честно признаться, что главным драйвером развития ИБ являются, в первую очередь, не объективные угрозы, а рынок и продажи (в свою очередь, только косвенно зависящие от тех самых угроз).

В этом контексте хотелось бы подвести некоторую черту и оценить современный (существующий) рынок ИБ с целью поиска наиболее эффективных, инновационных решений ИБ для службы SOC. При этом, разумеется, я не беру в расчет комплекс необходимых и уже традиционных технических мер (межсетевые экраны, антивирусы, сканеры уязвимостей, системы предотвращения вторжений и некоторые другие), которые хорошо зарекомендовали себя лет двадцать назад и остаются актуальными, по-прежнему эволюционируя. Точно так, как и не говорю о специализированных решениях для защиты конкретных систем (защита баз данных и Web,honeypot и др.). Ниже мой список наиболее эффективных, в ряде случаев «must have» решений и технологий SOC:

1. Появление в лог-серверах корреляционных механизмов и алгоритмов определило новую эру в системах управления и мониторинга информационной безопасности. В результате появился класс продуктов SIEM. SIEM способен в десятки раз ускорить как обнаружение инцидентов, так и их расследование. SIEM кардинальным образом повышает эффективность ИБ — это тот случай, когда найден способ отдать машине рутинные операции, оставив человеку лишь аналитику. Именно поэтому, SIEM стал вычислительным «мозгом» и основным инструментом SOC.

2. Поведенческий анализ сетевого трафика в системах обнаружения вторжений. Сигнатурные механизмы могут быть эффективными, однако целый пласт zero-day атак и DDoS-атак они детектировать не способны. Сейчас поведенческие механизмы обнаружения атак реализуются в большом количестве продуктов, определив новый класс решений Next Generation IPS и системы защиты от DDoS. В корпоративной, банковской среде — это один из самых эффективных механизмов ИБ, направленных против пресловутых APT атак. Для SOC эти продукты могут стать незаменимыми инструментами обнаружения zero-day и расследования инцидентов.

3. Системы мониторинга действий пользователей и администраторов. Принципиально новый класс продуктов, позволяющий службе SOC получить дополнительные инструменты предотвращения, мониторинга и расследования инцидентов, в первую очередь, в случае реализации угроз через векторы атак со стороны внутреннего злоумышленника.

4. Ботнет-фильтрация. Простой и изящный механизм, позволяющий SOC-команде оперативно детектировать и нейтрализовать свершившийся факт заражения узла. Несмотря на простоту реализации, потребовал определенного периода повышения уровня зрелости продуктов ИБ, связанных с регистрацией и блокированием управляющего трафика ботнет и сбора базы данных по CC-серверам.

5. Системы однонаправленной передачи данных (они же диоды данных). Единственные решения, сертифицированные ISO/IEC Common Criteria по уровню EAL7 (Evaluation Assurance Level 7), что, по сути, означает гарантированную защиту периметра от внешних угроз ИБ (ни одно другое техническое решение ИБ не обеспечивает такой гарантии, потому что диоды данных делают это на аппаратном уровне). Системы однонаправленной передачи данных полностью изолируют критичный сегмент, сохраняя необходимый уровень взаимодействия со смежными системами. Это может быть востребовано в SOC, например, для безопасного сбора событий или копий трафика из критичных сетей и их сегментов (не подвергая их рискам при подключении к внешним каналам связи) для дальнейшего анализа.

6. SI (Security Intelligence) — аналитика в SOC. Новый подход, который, в частности, используется в услуге компании АМТ-ГРУП (сервис АМТ SOC). Как правило, служба SOC оперирует фактами на языке ИБ (события, инциденты), получая эти данные в виде отчетов и визуализированных гра-

фиков со стороны SIEM. Однако для бизнеса и топ-менеджеров такое представление на оперативном уровне не всегда (почти никогда не) является информативным, показательным и определяющим необходимость каких-то действий. SI позволяет получить более высокий уровень корреляции событий и инцидентов ИБ с бизнес-процессами компании, данными от HR (например, новые сотрудники или уволенные сотрудники), СКУД, бухгалтерии и других бизнес-систем. Этот подход требует квалифицированной работы для создания модели данных со стороны бизнес-аналитиков компании и специалистов SOC. При этом на выходе, со стороны руководства, мы получаем немаловажное понимание эффективности службы ИБ и необходимости трат на ИБ.

7. OpenSOC. Когда мы говорим о SOC регионального уровня (уровня города, крупной международной корпорации) с сотнями тысяч пользователей и источников событий, то на первое место выходят новые вызовы для SOC. Такие масштабы характеризуются огромным количеством системных событий и событий ИБ, исчисляющихся (ежедневно) триллионами, миллиардными показателями Flow per Second статистики, терабайтами переданного трафика. Два главных технологических вызова SOC при таких масштабах: необходимость оперировать действительно большими базами данных (индексация, хранение, поиск) и необходимость создавать корреляционные правила для огромной инфраструктуры. Концепция OpenSOC (open source решение, продвигаемое компанией Cisco Systems) воспринимает информацию от различных источников событий (сетевой трафик, статистика Flow, события и т.д.) — как телеметрию (т.е. огромный поток входных данных BigData). Процесс парсинга, форматирования, индексирования и выявления инцидентов в терминологии OpenSOC называется обогащением (enrichment) и при этом используются технологии BigData, разработанные под масштабирование высокого уровня. Но какую бы производительную платформу с высокоскоростным индексированием и поиском мы не использовали, SOC командам понадобилась бы целая армия квалифицированных специалистов для оперативного создания корреляционных правил — дело в том, что на больших масштабах инфраструктуры инциденты новых типов могут возникать быстрее чем SOC-команда будет успевать их идентифицировать и определять в корреляционных правилах. Для решения этой задачи OpenSOC использует технологию поведенческого событийного анализа для прогнозного моделирования возможных инцидентов. Другими словами, все возможные элементы рутинных операций, включая поведенческий событийный анализ, уже отдаются машине.

* * *

По отдельности элементы такого решения в той или иной форме начинают развиваться в существующих SIEM. Однако, OpenSOC эффективно решает эту задачу на принципиально ином уровне и в других масштабах в сравнении с традиционными SIEM — примерно, как крупная ГЭС отличается от водяной мельницы при схожих принципах работы. Кто знает, может когда-нибудь, подобная концепция будет реализована в глобальных национальных системах типа ГосСОПКА?

Денис ДЫГИН

эксперт Технического комитета по стандартизации ТК 26, член рабочей группы Государственной Думы Федерального Собрания РФ по вопросу правового регулирования выпуска и оборота криптовалюты

Иван ЛАВРИКОВ

эксперт Технического комитета по стандартизации ТК 26, эксперт ISO TC 307 "Blockchain and electronic distributed ledger technologies"

Григорий МАРШАЛКО

эксперт Технического комитета по стандартизации ТК 26, эксперт ISO TC 307 "Blockchain and electronic distributed ledger technologies", член рабочей группы Государственной Думы Федерального Собрания РФ по вопросу правового регулирования выпуска и оборота криптовалюты

Василий ШИШКИН

эксперт Технического комитета по стандартизации ТК 26, эксперт ISO TC 307 "Blockchain and electronic distributed ledger technologies", кандидат физико-математических наук

ЭЛЕКТРОННЫЕ ВАЛЮТЫ

Технические и нормативные вопросы функционирования и обеспечения безопасности

Широко обсуждаемый в настоящее время феномен «электронных валют» или, как их еще называют, «криптовалют», зачастую трактуется неоднозначно. Под электронной (крипто-) валютой различные авторы, да и финансовые институты, часто понимают и универсальный финансовый инструмент, и средство накопления, и товар, и, что наиболее распространено, электронные денежные средства, которые используются как «альтернативная» или «дополнительная» валюты.

На основе информации, содержащейся в доступных источниках, можно сделать вывод, что идея создания криптовалют возникла в 1998 году. В работах Вэй Дай рассматривается возможность построения денежной системы для общества, пребывающего в состоянии так называемой «криптографической анархии» (англ. *crypto-anarchy*), концепция которой была сформулирована в 80-х годах прошлого века Тимоти Меем в «Манифесте криптографического анархиста». Правительства, регулирующие и надзорные органы в данном обществе являются избыточными элементами. Идеология «криптографической анархии» основывается на вере в стойкость используемых криптографических механизмов, широкое распространение которых, по мнению автора, и позволит обеспечить невозможность проведения со стороны государства (или другого контролирующего органа) ревизионных мероприятий в отношении содержания или характера передаваемой между субъектами информации, равно как и личностей указанных субъектов. Подобная концепция, с одной стороны, позволила сформулировать условия задачи (в том числе, криптографической) по построению систем выработки и обмена «де-

нежными единицами» без участия контролирующих органов (сейчас уже сложно представить себе общество без денег или их эквивалента). С другой стороны, сформировался определённый круг лиц, заинтересованных в создании и использовании подобных систем (в частности, лиц, стремящихся скрыть свою финансовую деятельность). Существенное развитие информационно-телекоммуникационных систем открыло дополнительные возможности оборота таких «денежных средств», поскольку расширило круг лиц, которые могут их использовать.

Если отойти от вопроса регулирования финансовой составляющей и рассмотреть непосредственно технические аспекты, то становится очевидным, что реализация криптовалюты представляет собой некоторую информационную систему, в которой пользователи обрабатывают определенный тип информации. Данные информационные системы обычно предназначены для эмиссии, обмена и учёта некоторого цифрового актива. При этом ключевыми представляются механизмы осуществления транзакций между пользователями системы, подтверждения транзакций (и обеспечения невозможности отказа от совершённой транзакции), хранения истории транзакций. Для реализации данных механизмов обычно используются функции:

- ♦ регистрации пользователей системы (с проведением или без проведения процедуры (упрощённой) идентификации);
- ♦ эмиссии и/или изъятия из обращения используемого цифрового актива;
- ♦ передачи информации, её обработки, хранения и подтверждения подлинности.

Вне зависимости от законодательного отношения к криптовалютам, можно утверждать,

что циркулирующая в системе криптовалюты (или какой-либо другой системы, построенной по сходному принципу) информация обладает определённой ценностью для пользователя. В связи с этим, важнейшим аспектом является обеспечение безопасности информации при её передаче, обработке и хранении. Следует отметить, что в настоящее время в Российской Федерации уже существует устоявшаяся законодательная и нормативная база в области защиты информации. Она определяет широкий спектр вопросов как в чисто техническом (например, использование определенных алгоритмов, форматов данных и т.п.), так и в организационном (сертификация систем, учет носителей и т.п.) планах.

В частности, в системе, как правило, циркулирует информация о пользователях, например, сведения, используемые при идентификации, и история транзакций. Особенно остро вопрос обеспечения безопасности подобной системы может встать в случае, если потребуется реализация механизмов аутентификации пользователей в системе. Таким образом, при реализации данных систем необходимо принимать во внимание положения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Нельзя забывать, что любое решение в области безопасности разрабатывается в рамках некоторой теоретической модели, поэтому, в случае, если реальная ситуация его использования будет отличаться от такой модели, то, как показывает современная практика исследований, оно уже не может дать полной гарантии защищённости. Действительно, использование криптографических систем с теоретически обоснованными свойствами не всегда приводит к требуемому результату.

Рассмотрим простой пример. Пусть есть руководитель, наделённый возможностью ставить электронную подпись под документом, и его секретарь, который данный документ для подписи предоставляет. В случае, если секретарь является доверенным лицом, то руководитель может быть уверен в том, что содержание предоставленного документа соответствует представлению о нём. В противном случае, секретарь может модифицировать содержание документа и, при отсутствии у руководителя достаточно количества времени для изучения всех подготавливаемых документов, получить для него

электронную подпись руководителя. Отметим, что при разработке схем электронной подписи подобные угрозы также могут быть приняты во внимание, но, во-первых, создание мер противодействия им может привести к существенному усложнению используемого математического аппарата и удорожанию системы в целом, а во-вторых, подобное требование может просто не учитываться, исходя из действующего в законодательстве определения электронной подписи.

Приведенный пример наглядно демонстрирует, что само по себе использование криптографического алгоритма и протокола не является достаточным для всестороннего обеспечения безопасности. Именно поэтому возникает большой набор дополнительных организационных и технических требований, цель которых — максимально приблизить реальные условия использования криптографического алгоритма к условиям теоретической модели. В совокупности все сказанное и составляет то понятие, которое принято называть информационной безопасностью.

Таким образом, только при комплексном применении, методы защиты (законодательные, организационно-технические, криптографические и др.) позволяют гарантировать безопасность информации. Именно поэтому, например, в рамках Федерального закона от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи», который является законодательным методом защиты, указываются требования к криптографическим методам, а также к их технической реализации и применяемым организационным мерам. Более того, в случае электронной подписи конкретные механизмы обеспечения безопасности определяются свойствами конкретного нормативного понятия/процесса.

Насколько озвученные моменты учитывались при создании криптовалют — вопрос открытый. Проведенные к настоящему времени исследования показывают, что модели угроз, которые исходно рассматривались, далеко не в полной мере отвечают угрозам, возникающим при при-

Использование криптографических систем с теоретически обоснованными свойствами не всегда приводит к требуемому результату

Статья подготовлена по результатам выступления авторов на Международной научно-практической конференции «Электронная валюта в свете правовых и экономических вызовов», прошедшей в июне 2016 года в Государственной Думе Федерального Собрания РФ.

менении криптовалют в глобальной мировой информационно-телекоммуникационной среде. Равно как и внедрение механизмов взаимодействия с подобными валютами в современные информационно-телекоммуникационные системы также не было рассмотрено. Анализируя научные публикации, связанные с рассматриваемой областью и подготовленные за последние четыре года, можно сделать вывод о том, что только сейчас начинает зарождаться общая формализованная методология создания и оценки безопасности систем подобного назначения. Результаты этих исследований во многом являются вызовами для безопасности и стабильности функционирования существующих в настоящее время систем криптовалют. Предстоит пройти долгий путь до того момента, когда специалисты в области криптографии и информационной безопасности создадут такой же строгий аппарат оценки свойств криптовалют, какой существует в настоящее время, например, для криптографических примитивов.

Сейчас же вдохновлённые идеями «криптографической анархии» разработчики технологий криптовалют не до конца отдают себе отчёт в том, что использование только криптографических механизмов не всегда может обеспечить требуемый уровень безопасности в конкретных приложениях. Более того, для полноценного

перехода общества в состояние «криптографической анархии», в целом, потребовалась и до сих пор требуется разработка новых криптографических механизмов, а их состоятельность покажет только время и дополнительные независимые, всесторонние технические, математические и криптографические исследования. С другой стороны, условия применения классических механизмов в системах подобного типа, в ряде случаев, совершенно не согласуются с задачами, для которых указанные механизмы создавались.

* * *

В заключение отметим, что вопрос о повсеместном использовании электронных (крипто-) валют, связан не только с необходимостью разработки строгого понятийного и научного аппаратов, позволяющих осуществлять адекватное описание и оценку уровня безопасности разрабатываемых решений, но и с концептуальным переосмыслением роли и функций государственных и/или регулирующих институтов в условиях существования такого независимого от них объекта, как криптовалюта, а в конечном итоге, возможно, роли и функций государства как такового.



БЛОКЧЕЙН — НАЧАЛО ПУТИ

Некоторое время назад блокчейн взорвал информационное пространство в ИТ. Появились конференции, рабочие группы, объединения и заявления авторитетных участников индустрии. Это породило верных последователей, и, конечно, критиков и скептиков. Последние называют первых «свидетелями блокчейна», а советник президента Клименко даже называл блокчейн «мозговым вирусом». Но в итоге и он сдался, включив блокчейн в повестку своих конференций.

Такая поляриность мнений вполне объяснима — изящность изобретения будоражит воображение, но массового применения технологии пока не произошло. Что же его останавливает?

Перед тем, как ответить на этот вопрос, давайте попробуем разобраться, что из себя представляет эта технология. В первую очередь — это децентрализованная система хранения важных данных, где каждый из пользователей может доказать, что он ими владеет и может передать их другому. Наиболее понятно это работает с криптовалютами — пользователи хранят в системе «деньги» — по сути запись о принадлежащих им монетах — и могут передать их другому. Копии этих записей хранятся у всех участников в виде последовательной цепочки блоков, где каждый последующий блок содержит информацию о предыдущем (собственно эта часть технологии и дала общее название — блокчейн, то есть цепочка блоков). Таким образом пользователи могут быть уверены, что данные не будут изменены.

Важное качество, которое можно заметить — пользователи не зависят друг от друга или от центрального звена. Это дает им независимость, а системе — устойчивость.

Что это может дать нам на практике? Например, можно хранить наличные в цифровом виде, или данные о страховке или регистрации недвижимости. В такой системе легко проводить расчеты и к ней удобно подключиться.

Почему же это не работает уже сейчас?

Из-за молодости этой технологии она пока еще недостаточно производительна, существующие популярные реализации работают очень медленно, и не позволяют проводить больше 7–15 транзакций в секунду (для примера, в пике у Киви количество транзакций может достигать

900 в секунду). Правда, на заре интернета он тоже не позволял качать видео в HD качестве, поэтому технологически эту задачу скорее всего удастся решить.

В финтех-среде еще сохраняется скепсис в отношении применимости данной технологии — не является ли она очередным модным веянием? И здесь мы опять сталкиваемся с классическим вопросом «курица или яйцо» — без технологии нет прототипов, без прототипов нет технологии.

Большее число мировых финансовых институтов на этот вопрос уже ответили. А именно, создали консорциум R3, в рамках которого проводятся R&D разработки.

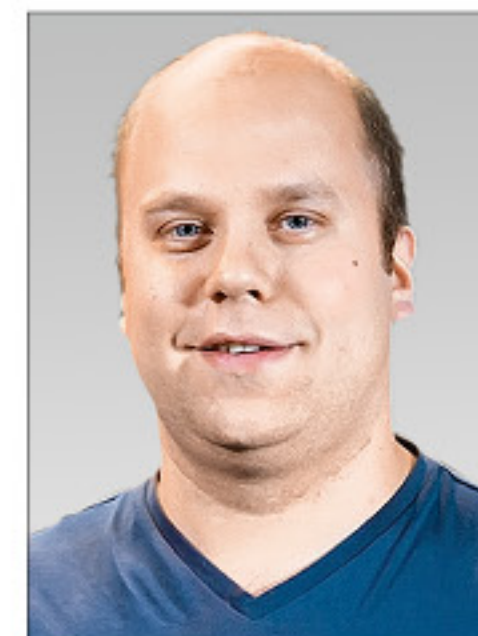
Ответили на него и многие участники российского финтех-рынка, в том числе и QIWI, запустив в тестовом режиме криптопроцессинг. Поэтому уже можно говорить о сложившемся тренде. Вопрос только в сроках перехода от стадии прототипирования к стадии внедрения (которая уже началась). Остальным участникам останется выбрать: либо принять участие в этом стриме, либо дождаться момента, когда их будут вовлекать в уже созданные технологии.

Вторая существенная проблема — это встраивание системы распределенного хранения реестров в существующую систему отношений и регулирования. При распределенном оперировании реестром и ответственность распределена между участниками, и пока только предстоит придумать, как решить эту проблему.

Мы сейчас очень много действий совершаем в цифровом мире, но права нашей цифровой личности, ее идентификация и возможности ограничены старыми представлениями и технологиями. Каждый участник рынка проводит идентификацию по своим правилам, это регулируется разными законами и это не может быть использовано для разных задач.

Однако, если эти задачи смогут быть решены, появится возможность безопасного хранения ваших денег и данных без бумажных носителей, например, в телефоне, когда не нужно будет носить карточки, идентификационные документы и бумажные купюры.

Несмотря на скепсис и молодость технологии сегодня, наконец, стало понятно, как это может реализоваться.



Алексей АРХИПОВ
директор по развитию
новых технологий
компании QIWI



Константин КОЛЬЦОВ
директор
по корпоративным
отношениям
компании QIWI



СЕКРЕТЫ ВРЕДОНОСНОГО КОДА

Исследования последних SWIFT-атак на зарубежные банки позволяют выяснить особенности вредоносного ПО и усилить защиту информационных систем

За последние несколько лет крупные банки различных стран подверглись атакам, в ходе которых при проведении мошеннических транзакций использовалась межбанковская система передачи информации и совершения платежей SWIFT. В результате проведенных расследований экспертам удалось получить детальную техническую информацию, касающуюся особенностей функционирования вредоносных программных средств, внедренных злоумышленниками. Указанная информация позволяет сформулиро-

вать некоторые рекомендации, направленные на повышение уровня информационной безопасности банков.

ВОЛНА SWIFT-АТАК НАБИРАЕТ СИЛУ

В феврале 2016 года злоумышленники попытались похитить 951 млн долларов путем направления фальсифицированных платежных поручений из Центрального банка Бангладеш в Федеральный резервный банк Нью-Йорка. Хотя большинство транзакций было приостановлено, банк лишился 81 млн

долларов. После появления в СМИ результатов экспертного анализа этого крупнейшего инцидента в поле зрения специалистов оказались также аналогичные атаки, проведенные против кредитно-финансовых учреждений в других странах. Все они были связаны с внедрением в банковские информационные системы вредоносного ПО и с хищением денежных средств с использованием системы SWIFT.

Одной из первых жертв подобных атак стал бангладешский банк Sonali Bank, потерявший в 2013 году 250 тыс. долларов. В январе 2015 года со счетов

эквадорского банка Banco del Austro было украдено 12 млн долларов. В октябре того же года была проведена атака против одного из филиппинских банков. В декабре 2015 года мошенники пытались украсть более 1 млн долларов со счетов вьетнамского акционерного коммерческого банка Tien Phong Bank (TPBank), но потерпели неудачу. В июне 2016 года стало известно о краже 10 млн долларов из неназванного украинского банка. Список пострадавших банков можно легко продолжить.

Чтобы правильно выстроить линию обороны против подобных атак, необходимо провести анализ методов и средств, которыми воспользовались злоумышленники для достижения своих целей.

ХРОНИКА СОБЫТИЙ В ДАККЕ

Когда один из руководителей Центрального банка Бангладеш Зубер Бин Худа (Zubair Bin Huda) в пятницу, 5 февраля, пришел в офис, оказалось, что выходной лоток принтера, расположенного в серверной комнате, был пуст. Поэтому он и другие сотрудники банка были лишены возможности получить информацию о транзакциях за предыду-

Успеху атаки способствовало еще и то обстоятельство, что в сети бангладешского банка не был установлен межсетевой экран и использовались дешевые маршрутизаторы, стоимостью около 10 долларов каждый

щий день. Когда Бин Худа попытался вручную распечатать подтверждения о транзакциях, ему это не удалось. Поскольку пятница в Бангладеш — выходной день, он ушел с работы пораньше, попросив коллег устранить неполадки с принтером.

Когда на следующий день, в субботу, 6 февраля, Бин Худа снова вышел на работу, он обнаружил, что программное обеспечение терминала, подключенного к системе SWIFT, не функционирует. После перезагрузки на терминале появилось предупреждение о том, что один из файлов отсутствует или изменен. К середине дня сотрудникам все же удалось запустить терминал и вручную распечатать информацию о транзакциях. К своему удивлению они обнаружили десятки сообщений, содержащих

запросы в Федеральный резервный банк Нью-Йорка на переводы денежных средств на счета в третьих странах.

Только 8 февраля сотрудниками банка было полностью восстановлено подключение к системе SWIFT. Тогда они обнаружили подозрительные транзакции на общую сумму 101 млн долларов и направили в банки США, Филиппин и Шри-Ланки указания о блокировке мошеннических переводов денежных средств. Но было уже поздно. Указанные транзакции, инициированные злоумышленниками, были успешно выполнены.

Как выяснилось, 20 млн были переведены в Шри-Ланку, а 81 млн долларов был перечислен на четыре банковских счета на Филиппинах якобы с целью оплаты бангладешских инфраструктурных проектов, включая строительство мостов, электростанции и метро в Дакке. Впоследствии стало известно, что указанные денежные средства, в конечном итоге, были переведены на счета нескольких организаций игорного бизнеса на Филиппинах и обналичены.

Время для проведения указанной атаки было выбрано злоумышленниками не случайно. Воскресенье, 7 февраля, было в Бангладеш первым рабочим днем недели. Но этот день, также как и предыдущий, был выходным в американских банках. Поэтому сотрудникам Центрального банка Бангладеш не удалось связаться со своими американскими коллегами ни в субботу, ни в воскресенье. Кроме того, на Филиппинах, где много бизнесменов китайского происхождения, в понедельник, 8 февраля, отмечался Новый год по китайскому календарю.



Эквадорский банк Banco del Austro, со счетов которого было украдено 12 млн долларов

ТЕХНИЧЕСКИЕ ДЕТАЛИ ИНЦИДЕНТА

Корреспондентам агентства Reuters стали известны от специалистов компании BAE Systems некоторые технические детали произошедшего в ЦБ Бангладеш инцидента. Если утверждение экспертов BAE Systems о том, что «вредоносная программа зарегистрировала себя в качестве службы и действовала в среде SWIFT Alliance на платформе Oracle Database» соответствует действительности, то в таком случае большая часть вины за инцидент лежит на организации SWIFT.

Эксперты компании BAE Systems указали, что использованное в ходе атаки вредоносное ПО обладает способностью читать и модифицировать сообщения системы SWIFT, а также отправлять информацию на удаленный управляющий сервер. Кроме того, они полагают, что примененное злоумышленниками вредоносное ПО состоит из различных программных модулей, которые могли быть использованы при атаке на другие банки.

Хеш-значение MD5 исполняемого файла с вредоносным кодом в компьютерной системе Центрального банка Бангладеш не должно было позволить осуществить процесс его регистрации, загрузки в память и последующего выполнения без обнаружения системой защиты. Вредоносный код, в принципе, не должен был выполняться, а персонал, отвечающий за безопасность SWIFT, сразу же получил бы сигнал об атаке. По всей вероятности, имеющаяся уязвимость в клиентском программном обеспечении Alliance Access позволила злоумышленникам успешно внедрить вредоносный код в компьютерную систему банка и использовать его в своих целях.

Успеху атаки способствовало еще и то обстоятельство, что в сети бангладешского банка не был установлен межсетевой экран и использовались дешевые маршрутизаторы, стоимостью около 10 долларов каждый. После проникновения в сеть банка злоумышленники по-



лучили доступ к учетным данным системы SWIFT и вошли в нее, а затем смогли установить вредоносное ПО и провести мошеннические транзакции.

СТРУКТУРА ВРЕДОНОСНОГО КОДА

Как показали результаты проведенного экспертами расследования, вредоносные программные средства, использованные злоумышленниками при атаке на Центральный банк Бангладеш, включали в себя несколько исполняемых файлов и один конфигурационный файл, содержимое которого было зашифровано по криптоалгоритму RC4. Один из модулей вредоносного ПО был предназначен для изменения сообщений системы SWIFT. Другой модуль позволял злоумышленникам осуществлять удаленное подключение к компьютерной системе банка. Некорректная работа принтера была вызвана третьим модулем, входящим в состав вредоносного ПО. Его основная функция заключалась в уничтожении содержимого подтверждающих сообщений системы SWIFT перед их отправкой на печать.

При создании вредоносного ПО, использованного при совершении атак в Бангладеш и Вьетнаме, злоумышленники использовали среду разработки приложений Visual C++ 6.0 корпорации Майкрософт. Компиляция использованного для совершения атаки вредоносного кода была произведена незадолго до начала атаки.

ЧТО ПОКАЗАЛ ЭКСПЕРТНЫЙ АНАЛИЗ

Компании Symantec удалось обнаружить доказательства того, что атака

на филиппинский банк была подготовлена той же самой группой злоумышленников, которая похитила 81 млн долларов из Центрального банка Бангладеш и пыталась украсть более 1 млн долларов из вьетнамского банка TP-Bank. Во всех трех случаях, как установили эксперты, применялось вредоносное ПО, созданное этой группой. Некоторые особенности вредоносного программного кода, использованного злоумышленниками, по мнению экспертов Symantec, указывают на хакерскую группу Lazarus. Эту группу подозревают в причастности к кибератакам на компании в США и Южной Корее.

Компания Symantec провела детальный анализ вредоносных программных средств, использованных в ходе нескольких атак против финансовых организаций в Юго-Восточной Азии. При анализе были обнаружены фрагменты кода, предназначенного для перезаписи содержимого отдельных файлов. Указанный код обладает некоторыми отличительными признаками. Реализованная в нем процедура уничтожения файлов имеет два параметра: путь к файлу, который будет перезаписан, и количество итераций перезаписи. При выполнении вредоносной программы производится замена последнего байта файла. Для определения местоположения других перезаписываемых байтов использовались шесть «управляющих» байтов. Хотя на первый взгляд исходный код программы выглядел уникальным, экспертам удалось обнаружить такую же комбинацию «управляющих» байтов в других вредоносных программах. Уничтожение файла происходило следующим

образом. Вначале в файл записывался набор случайных символов, после чего он переименовывался и удалялся с жесткого диска.

Как выяснили зарубежные эксперты, во вредоносных программных средствах, обнаруженных в Центральном банке Бангладеш и во вьетнамском банке, был реализован описанный выше способ уничтожения файлов. Это было сделано для того, чтобы удалить следы атаки и затруднить проведение расследования.

ТРОЯНСКИЙ КОНЬ В ХАНОЕ

При атаке на вьетнамский банк использовался файл, представляющий собой троянскую версию распространённой программы для чтения PDF-файлов компании Foxit Software. В ходе атаки происходила установка вредоносного ПО в директорию, созданную при установке оригинального ПО Foxit, а затем осуществлялась замена названия файла с троянской программой на FoxitReader.exe, соответствующее названию оригинального файла. Как только пользователь ПК запускал указанный исполняемый файл, происходил запуск вредоносного кода и осуществлялась запись информации в некоторый лог-файл, расположенный в директории временных файлов. Анализ указанного лог-файла показал, что информация в нём, так же как и в Центральном банке Бангладеш, была защищена шифром гаммирования с коротким периодом.

Эксперты обратили внимание на присутствие во вредоносном коде некоторого списка, содержащего SWIFT-коды банков различных стран. Среди них — банки Австралии, Вьетнама, Италии, Кореи, Сингапура, США и Японии. Во вредоносном ПО, обнаруженном как во Вьетнаме, так и в Бангладеш, содержался SWIFT-код банка-жертвы. В частности, вредоносный код из вьетнамского банка содержал комбинацию символов TPBVNVX, представляющих собой SWIFT-код TPBank.

Если бы в Центральном банке Бангладеш осуществлялся мониторинг использования привилегированных учетных записей, аномальная активность была бы выявлена достаточно быстро

Примененные злоумышленниками программные средства способны просматривать заголовки сообщений SWIFT и проверять, содержится ли в них SWIFT-код отправителя сообщения, который «зашит» в список, находящийся во вредоносном конфигурационном файле. Как только находятся такие сообщения, происходит считывание содержащейся в них информации.

Кроме того, вредоносное ПО может производить различные манипуляции с сообщениями системы SWIFT: уничтожать информацию о транзакциях, стирать историю транзакций и содержимое системных журналов, препятствовать выводу на печать информации о совершенных мошеннических транзакциях.

В ходе дальнейшего анализа выяснилось, что во вредоносном коде была реализована функция преобразования PDF-файлов в XML-файлы. При этом использовался оригинальный драйвер из набора Foxit SDK. Преобразованные файлы сохранялись в специальной директории на жестком диске.

КАК ГОТОВИЛИСЬ ЗЛОУМЫШЛЕННИКИ

Проведение атак на банки Бангладеш и Вьетнама было тщательно подготовлено. Вполне вероятно, что злоумышленники воспользовались необходимой информацией, полученной от инсайдеров, работающих в этих банках. Вредоносный код, обнаруженный в Центральном банке Бангладеш, был разработан с учетом технических особенностей функционирующих в банке систем, включающих прикладное ПО, базы данных и принтер. Примененный во вьетнамском банке вредонос-

ный код также разрабатывался с учетом используемой программной среды. У злоумышленников была информация о том, что в банке применялся программный продукт компании Foxit Software.

У атакующих было очень хорошее понимание особенностей функционирования системы межбанковских сообщений SWIFT. Они знали, какие изменения нужно в нее внести, чтобы предотвратить обнаружение попыток хищения денежных средств.

В то же время при разработке вредоносного ПО злоумышленники допустили грубые орфографические ошибки. Ошибки содержались как в ПО, обнаруженном в Центральном банке Бангладеш, так и в ПО, внедренном в компьютерную систему вьетнамского банка.

ИЗВЛЕКАЕМ УРОКИ

Увеличение числа атак на банковские организации делает все более актуальной необходимость своевременного обмена информацией между участниками финансового сообщества, которая включала бы сведения о методах, применяемых злоумышленниками, о технических особенностях вредоносных программных средств и т.д. Такой обмен информацией о произошедших инцидентах будет способствовать выявлению слабых мест в защите банковских информационных систем и позволит выработать более эффективные меры информационной безопасности. В этой связи создание Центра мониторинга и реагирования на компьютерные атаки в финансовой сфере (FinCert) в Центральном банке Российской Федерации является важной и актуальной мерой

противодействия криминальной активности.

В ходе нападений на информационные системы атакующими многократно использовались привилегированные учетные записи системных администраторов и пользователей критичных банковских приложений. Это дало возможность злоумышленникам действовать внутри банковских компьютерных сетей и получать разрешения на переводы крупных денежных средств. Если бы в Центральном банке Бангладеш осуществлялся мониторинг использования привилегированных учетных записей, аномальная активность была бы выявлена достаточно быстро.

* * *

С учетом результатов экспертного анализа инцидентов кредитно-финансовым организациям России можно настоятельно рекомендовать предпринять необходимые шаги, чтобы помешать злоумышленникам получать внутренние идентификационные данные, необходимые при осуществлении доступа к информационным системам. Применение многофакторной аутентификации, система контроля и мониторинга за использованием привилегированных учетных записей, обнаружение потенциально опасной активности и быстрая реакция на сигналы тревоги должны быть в центре внимания служб информационной безопасности, чтобы снизить вероятность осуществления в дальнейшем подобных атак.



Евгений АФОНИН

директор департамента консалтинга и аудита компании «Информзащита»

В ситуации с атакой на Центральный банк Бангладеш показательны следующие факты:

... выходной лоток принтера был пуст... руководитель, не получив информацию о транзакциях за предыдущий день... ушел с работы ...

... программное обеспечение терминала, подключенного к системе SWIFT, не функционирует. После перезагрузки на терминале появилось предупреждение о том, что один из файлов отсутствует или изменен ...

... вредоносная программа зарегистрировала себя в качестве службы...

... не был установлен межсетевой экран...

... один из модулей вредоносного ПО был предназначен для изменения сообщений системы SWIFT...

... вредоносное ПО может производить различные манипуляции с сообщениями системы SWIFT...

Из перечисленных фактов можно сделать следующие предположения:

1) В банке отсутствуют или неконкретны технологические регламенты и не установлена ответственность сотрудников за их выполнение.

2) У персонала, ответственного за эксплуатацию аппаратно-программ-

ного комплекса (АПК) подключения к системе SWIFT, низкий уровень осведомленности по вопросам ИБ.

3) Отсутствует, либо неконкретен перечень инцидентов ИБ и порядок реагирования на инциденты ИБ.

4) Сегмент сети, в котором размещен АПК подключения к системе SWIFT, не изолирован от общей сети организации, а также не контролируется трафик.

5) В организации не реализованы процессы мониторинга событий ИБ и реагирования на инциденты.

У российских банков зачастую ситуация с информационной безопасностью очень похожа на описанную. Поэтому каждому банку необходимо провести оценку защищенности подключения организации к сети SWIFT, в том числе выполнить анализ:

♦ архитектуры подключения к сети SWIFT;

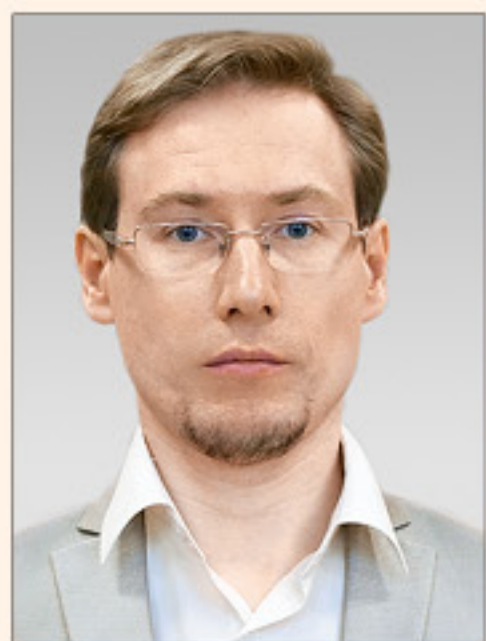
♦ конфигураций системных компонентов (операционных систем, прикладного ПО, сетевого оборудования, СЗИ), реализующих подключение к сети SWIFT;

♦ основных процессов ИБ;

♦ безопасности интерфейсов АПК SWIFT с другими банковскими информационными системами.

ЛИТЕРАТУРА

1. Printer Error Triggered Bangladesh Race to Halt Cyber Heist, Bloomberg, March 16, 2016
2. Bangladesh Bank hackers compromised SWIFT software, warning issued, Reuters, Apr 25, 2016
3. Vietnam bank says interrupted cyber heist using SWIFT messaging, Reuters, May 15, 2016
4. Now It's Three: Ecuador Bank Hacked via Swift, The Wall Street Journal, May 19, 2016
5. SWIFT hackers nick \$ 10m from Ukraine bank, the Register, Jun 28, 2016



Андрей ЗАХАРОВ
руководитель группы
информационной безопасности
компании «Инфосистемы Джет»

Произошедшие инциденты с участниками платежной системы SWIFT объединяет не только изощренность методов, используемых злоумышленниками, но и запредельный уровень халатности пострадавших банков. Понимая всю критичность ситуации, в июне 2016 года SWIFT разработала и представила общественности программу Customer Security Program (CSP), призванную переломить опасный тренд. Программа включает 5 инициатив, которые призваны устранить проблемы, послужившие причиной случившихся инцидентов.

В первую очередь, по мнению SWIFT, должен быть налажен обмен информацией об угрозах, признаках компрометации и мерах противодействия угрозам внутри SWIFT-комьюнити, а также создана команда оперативно реагирования на инциденты. Принцип «знай своего врага» поставлен во главе угла.

Вторым шагом предполагается усиление ключевых мер защиты клиентской SWIFT-инфраструктуры. Прежде всего, это защита информационных потоков между SWIFT AllianceAccess и бэк-офисными системами (АБС), где создаются электронные платежные сообщения. Другие меры включают усиленный контроль целостности программной среды, а также непрерывный мониторинг действий пользо-

вателей. Данные меры направлены на борьбу, в первую очередь, с таргетированными атаками.

В рамках третьего шага организации-участники SWIFT должны внедрить у себя лучшие практики обеспечения информационной безопасности, включая разделение полномочий и строгий контроль доступа. Для этого должны быть разработаны соответствующие стандарты и руководства по безопасности. Ряд документов по этому направлению уже появился. По замыслу разработчиков это должно помочь предотвратить инциденты безопасности, вызванные более банальными причинами.

Четвертый шаг предполагает развитие мер выявления признаков мошенничества при подготовке и отправке электронных платежных документов. Комплекс мер должен включать не только классические средства контроля транзакций (RMA), реализующие принцип Know Your Customer (KYC), но и инструменты обнаружения аномалий в отправляемых платежах наряду с интеллектуальными средствами анализа бизнес-контекста.

Заключительный пятый шаг программы предусматривает разработку комплекса требований безопасности к поставщикам услуг с целью общего повышения уровня зрелости экосистемы сервисов, так или иначе связанных с системой SWIFT.

В рамках пятого шага SWIFT планирует запустить программу сертификации поставщиков услуг, включая аудиторов информационной безопасности.

* * *

В результате реализации этой программы в перспективе мы должны будем увидеть экосистему, подобную той, которую выстроил вокруг международных платежных систем PCI Council.





ДЕЛО НЕ НА ОДНУ ПИЦЦУ

История расследования

Пока ещё прохладное июльское утро среды. В российском ИБ-мире традиционное летнее затишье. Сидим в офисе, пьем кофе и неспешно осваиваем новое ПО для анализа логов. И вдруг звонок от партнёра «Перспективного мониторинга» в одном из регионов: «Ребята, нашего заказчика, похоже, взломали. Тут вроде всё и очевидно, и как-то странно. Помогите разобраться». Заказываем билеты и в путь!

В любом расследовании инцидента информационной безопасности в первую очередь важно понять и выяснить кто, когда и как заметил, что инцидент произошёл или мог произойти. С этого человека и начинается расследование: как правило, если кто-то регулярно работает с информационным ресурсом, то лучше всех и понимает, как тот устроен и как должен нормально функционировать. Иногда заметить атаку очень просто — например, изменяется главная страница корпоративного сайта, или IDS фиксирует регулярные попытки перебора паролей, или пользователь получает «весёлое» сообщение криптолокера с требованием заплатить выкуп за данные. Иногда сложнее — компьютер внезапно стал тормозить, или вырос объём сетевого трафика.

На первый взгляд в нашем случае было как раз всё просто — сайт заказчика поменялся, хотя все редакторы и администраторы клялись, что не

трогали его. Простейшая логика подсказывала — если у нас есть предыдущее состояние информационной системы (Ура! Они делали бекапы!) и есть текущее состояние, то ответ на все наши вопросы хранится где-то в изменениях.

Важно понимать, что киберпреступления совершают люди. И они всегда оставляют следы своего присутствия в информационной системе — как бы они ни старались их уничтожить или замаскировать. И обычно эти следы находятся в логах, дампах памяти, результатах работы специального программного обеспечения форензики.

Мы сформировали поверхность атаки со всеми возможными векторами атак и гипотезами, начиная от уязвимостей CMS (системы управления контентом) сайта и заканчивая осознанными вредоносными действиями администратора сайта. Чтобы понять, что происходит в ИТ-инфраструктуре организации, надо самому ненадолго стать системным администратором. Мы на практике выяснили, что сисадмины пострадавшей организации могут подробно ответить на 4 листа наших вопросов всего за каких-то пару часов. Это существенно дольше одной пиццы или трубки, но ведь и Ш. Холмс — персонаж вымышленный, в отличие от сердитого руководства.

Благодаря этой сессии вопросов и ответов, мы смогли сократить число

возможных гипотез в несколько раз. В данном случае мы могли проверить оставшиеся предположения прямо на «боевой» системе без особого риска что-то поломать и повлиять на доступность сайта и сервисов, хотя, конечно, так бывает далеко не всегда и приходится воспроизводить узлы инфраструктуры на стендах. Так мы отбросили ещё несколько гипотез.

Оставшиеся варианты атаки имели одну общую черту — действия совершались от имени легитимного редактора сайта. Логи CMS и сервера также говорили нам, что сама платформа не подвергалась атакам в период, непосредственно предшествовавший взлому сайта. Пароли администраторов и редакторов сайта были сложные и длинные, не поддающиеся перебору. На сервере хранились только хеши с «солью». Следов использования рабочих эксплойтов на CMS мы также не смогли обнаружить. Сложив эти факты, мы пришли к выводу, что злоумышленник знал логин и пароль администратора сайта, и приняли эту версию как наиболее вероятную.

И тут мы попали в ситуацию, которую не любит никто — ни ИТ- и ИБ-службы, ни сами исследователи — нужно было осмотреться вокруг, потому что сайт стремительно переставал быть главной нашей проблемой. Профессиональная паранойя подсказывала, что атаке подвергся не только он.

На второй итерации, когда мы уже могли уточнять вопросы сисадминам и администратору сайта согласно нашей рабочей версии, мы выяснили, что учётные данные однажды пересылались электронным письмом. Похоже, кроме сотрудников организации, кто-то ещё читал их почту. Не очень хорошая новость для ИТ и безопасников, правда?

Важно понимать, что киберпреступления совершают люди. И они всегда оставляют следы своего присутствия в информационной системе — как бы они ни старались их уничтожить или замаскировать

ИТ- и ИБ-службы сделали то, что от них зависело — внедрили средства защиты информации и соблюдали базовые правила информационной безопасности. Просто иногда случаются успешные атаки

В логах почтового сервера мы смогли отыскать доказательства компрометации около 30 учётных записей. Каждую неделю на протяжении почти полугода сервер отдавал почту по запросу легитимного (с точки зрения сервера) пользователя на определённый IP-адрес. Таких IP-адресов было около десятка, и каждый использовался для получения писем 3–4 пользователей. По этому списку мы и стали копать дальше.

И в этот момент нам невероятно повезло! В логах прокси-сервера мы нашли один из этих «плохих» IP-адресов, к которому шли непонятные регулярные обращения по протоколу http. Если перевести с машинного языка на человеческий, то кто-то регулярно маячил наружу «я тут», «я тут», «я тут».

Следы привели нас на рабочее место системного администратора, на нём мы нашли троян, который и обращался к своему командному серверу. Что заставило злоумышленников получать почту на IP-адрес командного сервера, мы никогда не узнаем, но только благодаря этому просчёту мы смогли найти первопричину всех бед.

Исследователи «Перспективного мониторинга» в Москве провели реверс-инжиниринг вредоносного кода и смогли выяснить, что троян собирал метаинформацию обо всех офисных файлах, до которых мог дотянуться, упаковывал данные в зашифрованный архив и регулярно отсылал наружу. Анализ операционной и файловой систем компьютера показал, что троян попал на рабочую станцию через заражённый сайт.

Все логины и пароли почтовых учётных записей хранились в зашифрованном excel-файле на компьютере системного администратора. Мы пред-

положили, что троян с помощью кейлогера получил пароль от этого файла и отослал злоумышленникам, поскольку видели взаимодействие троянского ПО и управляющего сервера в логах сетевого оборудования. Теперь мы точно знали, что искать на других машинах.

После того, как мы собрали информацию об инциденте, заказчик расследования запустил процессы восстановления. Мы помогли вернуть работоспособность затронутых атакой информационных систем и ресурсов. После анализа результатов расследования мы порекомендовали поменять настройку и состав средств защиты информации, чтобы предотвратить повторение инцидента в будущем или закрыть наиболее критичный вектор атак.

В данном конкретном случае мы не нашли виноватых внутри организации, да перед нами и не стояло такой задачи — нас позвали установить, что произошло, обнаружить затронутые ресурсы и выяснить, какие данные были скомпрометированы. ИТ- и ИБ-службы сделали то, что от них зависело — внедрили средства защиты информации и соблюдали базовые правила информационной безопасности. Просто иногда случаются успешные атаки. Мы обнаружили новый вектор и помогли его ликвидировать. То же самое мы делаем и при комплексных тестах на проникновение в информационные системы, когда исследуем сайты и веб-приложения, СУБД, сетевые службы и сервисы (электронная почта, прокси, VoIP, FTP и пр.), сетевое обо-

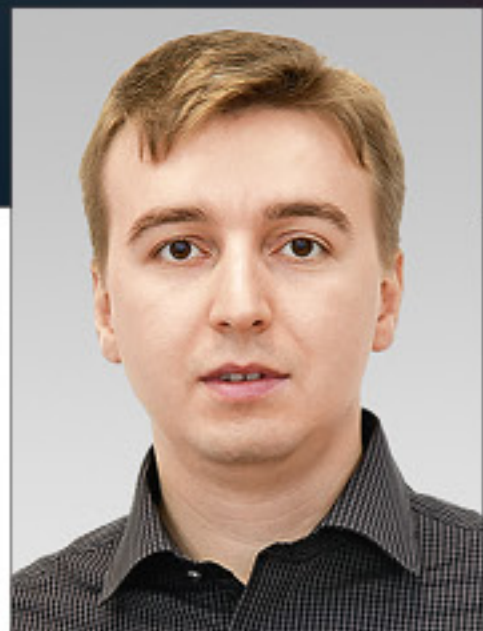
рудование, беспроводные технологии, средства защиты информации, серверные и пользовательские операционные системы, прикладное ПО.

Часто бывает ситуация, когда нужно понять долговременную логику действий нарушителя внутри информационной системы, выявить определённые закономерности поведения. Тогда мы устанавливаем у заказчика сенсоры IDS и подключаем их к нашему коммерческому Центру мониторинга, где аналитики уже могут спокойно наблюдать за развитием событий, разобраться, что происходит, и «разобрать» вредоносный код. Инцидент информационной безопасности может обнаружить дежурная смена центра мониторинга или к нам может обратиться непосредственно владелец ресурса, как было в описанном случае, если в его информационной системе есть подозрительная активность, при которой внедрённые ранее средства защиты информации «молчат». При этом в атакованной организации может не быть подготовленных и свободных ресурсов или опыта для расследования инцидента. И тогда «Перспективный мониторинг» может помочь — amonitoring.ru.

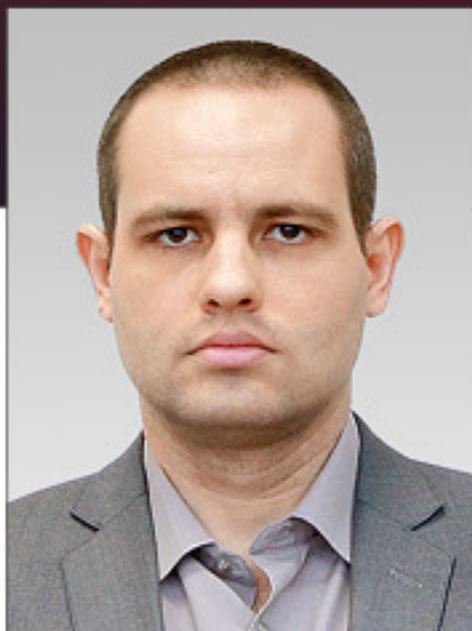


ЗАЩИТА ОТ ПОДДЕЛКИ ГОЛОСА В БИОМЕТРИЧЕСКИХ СИСТЕМАХ: СОВРЕМЕННОЕ СОСТОЯНИЕ ДЕЛ

*Девять из десяти способов подделки
голоса лишают смысла любое
применение голосовой биометрии
без детектора подделки*



Константин СИМОНЧИК
заместитель директора НИД
ООО «Центр Речевых
Технологий», к. т. н.



Дмитрий ЩЕТИНИН
руководитель управления
ООО «ЦРТ-инновации»,

Тема внедрения речевых технологий в системы обеспечения информационной безопасности банков, начатая нами ранее (статьи Ю. Н. Ромашкина и В. Н. Сорокина в № 1(4)/2012 и С. Ю. Мельникова в № 1(12)/2014), остается актуальной до настоящего времени. Речь является наиболее есте-



Рисунок 1. Общая схема атак на систему голосовой биометрии.

Безусловно, применение голосовой верификации дополнительно с другими традиционными средствами аутентификации повышает надежность системы информационной безопасности в целом. Однако всякое действие рождает противодействие. В настоящее время активно исследуются как способы повышения точности голосовой верификации, так и способы нападения на такие системы. Проблема устойчивости существующих систем верификации к подделке голоса рассматривается в публикуемой статье, которая позволяет оценить возможные риски аутентификации.

Биометрические технологии все чаще используются в системах безопасности для подтверждения личности человека или выявления мошенника. Так, например, некоторые банки не только в России, но и за рубежом проводят поиск изображения лица потенциального клиента по базам мошенников, голосовые контакт-центры используют голосовую верификацию звонящего с целью сокращения времени обслуживания клиента.

Действительно, принципиальным отличием биометрии является ее неотделимость от носителя — в отличие от пароля, аппаратного токена или электронно-цифровой подписи. Однако, действительно ли биометрические признаки нельзя подделать? В последнее время все большее количество потребителей биометрических систем озабочено не только качеством непосредственно биометрии, но и противодействием различным видам атак с целью получения доступа к защищенной информации (спуфинга). Так, например, изображение лица большинства клиентов банков можно найти в интернете — в социальных сетях или профилях организаций.

АТАКИ НА СИСТЕМЫ ГОЛОСОВОЙ БИОМЕТРИИ

В этой статье речь пойдет про биометрическую верификацию по голосу и современные способы детектирования подделки голоса.

Различают следующие виды атак на систему голосовой биометрии:

- 1) методы, основанные на приеме имперсонализации;
- 2) методы, основанные на записи голосовых биометрических характеристик человека и их дальнейшем повторе;
- 3) методы, основанные на технологии преобразования речи злоумышленника в речь другого человека;
- 4) методы, основанные на технологии синтеза речи.

Имперсонализацией называется процесс выдачи себя за другого человека. Применительно к голосовым биометрическим системам, такой вид атаки представляет собой наиболее простой и очевидный метод, основанный на имитации и изменении голоса путём подражания, без использования компьютерных технологий или специальных устройств [1]. Однако согласно исследованию, проведённому в работе [2], такой вид атаки не несет большой опасности, так как даже профессионалы пародии не в состоянии стабильно взламывать голосовые биометрические системы, основанные на устаревающих методах распознавания диктора и не содержащие каких либо решений по противодействию подобным атакам.

Самым очевидным способом фальсификации биометрических характеристик является их запись и повтор. В случае голосовых биометрических систем, злоумышленнику необходимо записать речь клиента биометрической системы и произвести попытку входа с использованием полученной записи.

ственным средством коммуникации, включая общение человека с машиной. Процесс порождения речи человеком является строго индивидуальным, в том числе и с точки зрения статистических характеристик сигнала, используемых при автоматической голосовой верификации пользователя.

Вероятность успеха подобной атаки очень сильно зависит от конструктивных особенностей голосовой биометрической системы. Например, при использовании текстозависимой системы верификации с динамической парольной фразой, схема работы которой изображена на рисунке 2, данный метод атаки применить невозможно.

Более серьезную угрозу для голосовых биометрических систем представляет техника голосовой конверсии или преобразования речи злоумышленника, в речь клиента биометрической системы. Техники голосовой конверсии модифицируют одно голосовое высказывание (источник), и звучат так, как будто произносятся другим диктором (целевым). Системы голосового преобразования состоят из этапа обучения и этапа преобразования. В обоих этапах речевой сигнал изначально разбивается на векторы признаков малой размерности. В обучающей фазе функции источника и целевого диктора вначале соединяются на уровне сегментов, обычно используются параллельные тренировочные высказывания. Функция преобразования в соответствии со стохастической моделью Гауссовых смесей (GMM) далее испытывается с использованием парных векторов [3]. На этапе конверсии функция преобразования используется для отображения скрытых факторов признаков, относящихся к целевому диктору. Конвертированное высказывание переделывается с использованием обратной параметризации.

Метод атаки на основе синтеза речи заключается в создании синтезированного голоса пользователя системы верификации. Для обучения системы синтеза используется предварительно записанная спонтанная речь пользователя. На этапе текстозависимой верификации, при помощи полученного синтезированного голоса и перехваченного парольного текста, создается синтезированная парольная фраза, используемая далее для попытки верификации. Эксперименты, проведенные в [4], показали, что при наличии



Рисунок 2. Схема работы текстозависимой системы голосовой биометрии с применением динамической парольной фразы

больших объемов речи целевого человека, система синтеза, обученная на этих данных, будет иметь высокое качество речи, плохо отличимое биометрическими системами от голоса живого человека (см. таблицу 1).

Однако для такого метода необходимы две составляющих: коллектив высококвалифицированных специалистов в области речевой обработки и речевая база с записями голоса целевого человека существенного объема. Подобная разработка доступна далеко не каждой группе злоумышленников, не говоря об одиночном человеке.

ПРОТИВОДЕЙСТВИЕ СПУФИНГ АТАКАМ

Большую работу в направлении исследования спуфинг атак на голосовые биометрические системы провела группа исследователей под руководством Tomi Kinnunen в Университете Восточной Финляндии. В 2015 году ими был организован первый в мире международный конкурс Automatic Speaker Verification Spoofing and Countermeasures (ASVspoof) Challenge 2015 [5] при крупнейшей конференции по речевым технологиям Interspeech. Результаты их исследований показали не только уязвимость голосовых биометрических систем к простейшим атакам на основе записи речи на диктофон, но и к более сложным способам синтеза голоса, а также к преобразованию голоса злоумыш-

Объем речи для обучения синтеза	Вероятность ложноположительной верификации (%)
1 минута	1,5
3 минуты	7,9
8 минут	19,1
30 минут	23,8
4 часа	98,4

Таблица 1. Вероятность пропуска злоумышленника при попытке атаки системой синтеза

ленника к заданному голосу пользователя системы.

Целью конкурса было не только оценить надежность существующих систем детектирования подделок голоса, но и в целом изучить существующие алгоритмы в этой области и перспективы их развития. Для того, чтобы максимально расширить круг участников, в качестве задачи ставилось только обнаружение факта подделки без детектирования типа подделки или интеграции детектора с голосовой биометрической системы. Участникам было предложено использовать любые данные, находящиеся в открытом доступе, для обучения своих систем. Но, кроме того, организаторами было предоставлено два дополнительных набора аудио данных:

1) набор записей «живой» речи 60 человек (всего 7247 записей);

2) набор записей подделок голоса указанных 60 человек, сгенерированных различными способами: с использованием синтеза речи, конверсии, склеек на базе различных алгоритмов (всего 62500 записей).

Участникам была предоставлена вся информация о каждой записи указанных наборов: идентификатор диктора, тип подделки голоса или информация, что голос является «живым».

Для оценки надежности качества детекторов подделки голоса была сформирована тестовая база из записей 46 человек: всего 9404 записи «живых» голосов и 184000 записи подделок. Информация о тестовых записях не раскрывалась, таким образом, учитывая объем файлов, участникам было крайне сложно повлиять на результат тестирования, используя ручную обработку.

Примечательно, что способы подделки голоса в тестовых записях отличались от способов, использованных в обучающем наборе. Таким образом организаторы хотели оценить устойчивость детекторов участников к неизвестным способам подделки голоса. Информация о способах подделки голоса приведена в таблице 2.

Чтобы подчеркнуть важность задачи детектирования подделок голоса для современных биометрических систем, организаторы привели результаты тестирования системы верификации по голосу, где в качестве эталона использовался голос живого человека, а в качестве тестового образца — результат конверсии с помощью приведенных выше способов. Результат сведен в таблицу 3.

Как видно, 9 из 10 способов подделки голоса лишают смысла любое применение голосовой биометрии без детектора подделки. Стоит, однако, учесть, что здесь аудио-сигнал подавался непосредственно в систему биометрии без искажений, которые могут возникать, например, при записи на диктофон. Воспроизведение с диктофона, поднесенного к телефонной трубке, существенно влияет на спектр сигнала и на практи-

Способ подделки голоса	Описание
S 1	Алгоритм на основе выбора сегментов речи из исходных записей
S 2	Конверсия голоса на основе подстройки первого мел-кепстрального коэффициента с целью подгонки наклона спектра речи к целевому голосу
S 3	Синтез на основе Скрытых Марковских Моделей, только 20 итераций адаптации
S 4	Тот же способ, что и S 3, но с 40 итерациями адаптации
S 5	Конверсия с помощью системы Festvox [6]
S 6	Конверсия голоса на основе максимального правдоподобия траекторий спектральных параметров [7]
S 7	То же способ, что и S 6, но с использованием линейных спектральных пар вместо мел-кепстральных коэффициентов
S 8	Конверсия голоса на основе тензорного представления в дикторском пространстве [8]
S 9	Конверсия голоса на основе алгоритма частичных наименьших квадратов [9]
S 10	Синтез речи с использованием открытого кода MaryTTS [10]

Таблица 2. Способы подделки голоса в тестовом наборе конкурса ASVspoof 2015

ке снижает вероятность успешной аутентификации при атаке таким образом.

Всего в конкурсе принимало участие 28 команд из 16 стран. Итоговые результаты участников, дошедших до финала, приведены в таблице 4.

Стоит отметить, что из России участие принимала только одна команда ООО «Центр речевых технологий», обозначенная под символом В и занявшая второе место в общем зачете.

Таким образом, с учетом активного развития речевых технологий, а также по итогам конкурса ASVspoof, современное состояние дел в области защиты биометрических систем от подделки голоса можно охарактеризовать следующим образом:

♦ в современном мире развиваются не только голосовые биометрические системы, но и способы подделки голоса, вариативность которых на сегодняшний день велика, а некоторые доступны в виде открытых кодов;

Способ подделки голоса	Равновероятная ошибка пропуска/отклонения, EER, %	
	Мужчины	Женщины
Без подделки	2,3	2,1
S 1	32,5	40,4
S 2	2,7	3,1
S 3	40,3	26,8
S 4	43,3	30,8
S 5	46,24	36,7
S 6	44,7	36,7
S 7	29,3	20,4
S 8	36,1	26,1
S 9	33,5	30,1
S 10	51,2	44,2

Таблица 3. Надежность типовой системы биометрической верификации по голосу на основе PLDA-подхода

♦ устойчивость биометрических систем к подделке голоса при определенных условиях низкая: большая часть способов подделки голоса может нанести серьезный урон качеству аутентификации;

♦ существуют подходы по распознаванию атак на биометрические системы, при этом большинство из них демонстрирует устойчивость к обнаружению способов конверсии и синтеза голоса, произведенных ранее не известным детектору методом;

♦ не только за рубежом, но и в России существуют команды разработчиков, способные эффективно реализовывать как сами биометрические системы, так и способы распознавания атак на них; в развитии и интеграции таких комплексных решений могут быть заинтересованы все потребители биометрических систем, особенно в случаях, когда пользователь проводит аутентификацию в удаленном или автоматическом режиме.

Команда	Равновероятная ошибка пропуска/отклонения, EER, %		
	Известные способы подделки	Неизвестные способы подделки	В среднем по всем способам
A	0,408	2,013	1,211
B	0,008	3,922	1,965
C	0,058	4,998	2,528
D	0,003	5,231	2,617
E	0,041	5,347	2,694
F	0,358	6,078	3,218
G	0,405	6,247	3,326
H	0,670	6,041	3,355
I	0,005	7,447	3,726
J	0,025	8,168	4,097
K	0,210	8,883	4,547
L	0,412	13,026	6,719
M	8,528	20,253	14,391
N	7,874	21,262	14,568
O	17,723	19,929	18,826
P	21,206	21,831	21,518
В среднем	3,337	9,294	6,316

Таблица 4. Результаты конкурса ASVspoof 2015

ЛИТЕРАТУРА

1. Lau Y. W., Wagner M., Tran D. Vulnerability of speaker verification to voice mimicking // Intelligent Multimedia, Video and Speech Processing, 2004
2. Mariéthoz J., Bengio S. Can a Professional Imitator Fool a GMM-Based Speaker Verification System? // IDIAP Research report IDIAP-RR 05-61. 2006. Mariéthoz J., Bengio S. Can a Professional Imitator Fool a GMM-Based Speaker Verification System? // IDIAP Research report IDIAP-RR 05-61. 2006.
3. Y. Stylianou, "Voice transformation: A survey," in Proc. Int. conference on acoustics, speech, and signal processing (ICASSP 2009), Taipei, Taiwan, April 2009, pp. 3585-3588.
4. Shchemelinin V., Topchina M., Simonchik K. Vulnerability of voice verification systems to spoofing attacks by TTS voices based on automatically labeled telephone speech // International Conference on Speech and Computer. — Springer International Publishing, 2014. — С. 475-481.
5. Wu, Z., Kinnunen, T., Evans, N., Yamagishi, J., Hanilçi, C., Sahidullah, M., & Sizov, A. (2015). ASVspoof 2015: the first automatic speaker verification spoofing and countermeasures challenge. Training, 10(15), 3750.
6. <http://www.festvox.org/>
7. T. Toda, A. W. Black, and K. Tokuda, "Voice conversion based on maximum-likelihood estimation of spectral parameter trajectory," IEEE Trans. Audio, Speech and Language Processing, vol. 15, no. 8, pp. 2222-2235, 2007.
8. D. Saito, K. Yamamoto, N. Minematsu, and K. Hirose, "One-to-many voice conversion based on tensor representation of speaker space," in Proc. Interspeech, 2011.
9. E. Helander, H. Silen, T. Virtanen, and M. Gabbouj, "Voice conversion using dynamic kernel partial least squares regression," IEEE Trans. Audio, Speech and Language Processing, vol. 20, no. 3, pp. 806-817, 2012
10. <http://mary.dfki.de/>

ДВА БЕРЕГА И-РЕКИ

Должна ли ИБ подчиняться ИТ?

«Искусство подчинять —
не разделить ли его на две части?»
Платон. «Диалоги. Софист»

«Для достижения устойчивости при переходе к цифровой модели, компаниям будет необходимо пройти фундаментальную организационную перестройку, в частности интегрировать кибербезопасность с бизнес-процессами и изменить способ управления ИТ».

James M. Kaplan. Beyond Cybersecurity. Protecting Your Digital Business

Если проследить эволюцию информационной безопасности, то мы увидим, что ИБ существовала задолго до появления вычислительной техники и информационных технологий. Многочисленные способы защиты информации хорошо известны — от узелкового письма инков, стратагем Сунь Тзы, криптографии в Византии и арабском мире, языка русских офицеров, говоривших слова задом наперед, вплоть до военной криптографии, появившейся в конце XIX века. Если взглянуть с точки зрения современных стандартов (например, ISO 27001), то мы увидим, что усилия наших предков, в основном, сосредотачивались на обеспечении конфиденциальности.

В конце 40-х годов, когда появились первые ЭВМ, информационная безопасность сводилась к охране зданий, в которых они находились (Physical Security).

Через полтора десятилетия, с появлением многопользовательских ОС, а затем вычислительных и автоматизированных телефонных сетей, проблема обеспечения информационной безопасности изменилась качественно. Новые ОС, СУБД и распределение вычислительных мощностей означали, что контроль периметра здания уже не мог обеспечить нужный уровень безопасности — доступ к информации можно было получить и без доступа в здание или машинный зал.

IT SECURITY

Ответом на новые вызовы явилось появление простейших функций аутентификации пользователей и разграничений прав доступа. Эти системы разрабатывались теми же программистами, которые разрабатывали ОС, СУБД и приложения. Естественно, что ответственность за эти функции легла на плечи тех же отделов, что управляли информатизацией предприятий. Так

информационная безопасность попала в область ответственности ИТ, что вполне отражалось в её названии — IT Security.

Примечательно, что в первом крупном документе, посвящённом информационной безопасности — RAND Report R-609-1¹, опубликованном в 1969 году, уже были чётко видны попытки отделить ИБ от ИТ в плане разделения обязанностей, была даже описана роль — Systems Security Officer. Но, как ясно видно из документа (раздел 'II. System Personnel'), назначалась эта роль Responsible Authority, двумя абзацами выше описывающаяся как «глава ИТ-департамента» («The head of the department or agency responsible for the proper operation of the secured computer system»).

Хотя уровень автоматизации бизнес-процессов предприятий (а особенно — финансового сектора) рос

¹ См. <http://www.rand.org/pubs/reports/R609-1/index2.html>



Константин СМЕРНОВ
CISA, CBSP, MBCI,
менеджер информационной
безопасности Accenture



Артём АГЕЕВ
CISSP, CEN,
MCSA:Security, консультант
по информационной
безопасности Accenture

Так как основные технические средства обеспечения ИБ — антивирусы, межсетевые экраны (брандмауэры), прокси-сервера — обслуживались ИТ, то логичной моделью взаимодействия ИТ и ИБ являлось подчинение ИБ департаментам ИТ

очень быстрыми темпами, коммуникационные сети не были доступны широкой публике. Примеры прогремевших в 1980-х Milwaukee 414s (взлом более 60 организаций, включая ядерную лабораторию в Лос-Аламосе), Кевина Митника в США с его ранними взломами телефонных и компьютерных сетей или Мурата Уртембаева в СССР, остановившего в 1983 году конвейер ВАЗа на 3 дня, незначительно способствовали повышению роли ИБ. До появления общедоступного Интернета в начале 90-х годов, а также возможности выхода в Интернет с помощью сотовых телефонов, информационная безопасность оставалась на заднем плане, будучи скорее ареной борьбы пользователей за права доступа.

Бум доткомов в 1999–2001 гг. и взрывообразный рост электронной коммерции, а затем — финансовых и государственных услуг, оказываемых через сеть Интернет, поставил компании перед фактом, что 99% процентов их бизнес-процессов зависят от информации, содержащейся в информационных системах и способности систем к обработке этой информации. Это вполне отразилось в новом названии — Information Security.

Так как основные технические средства обеспечения ИБ — антивирусы, межсетевые экраны (брандмауэры), прокси-сервера — обслуживались ИТ, то логичной моделью взаимодействия ИТ и ИБ являлось подчинение ИБ департаментам ИТ. На тот момент ИТ можно было уподобить архитекторам, а ИБ — пожарной охране. По сути это явилось развитием модели, принятой в начале 70-х годов XX века.

ЗА РАМКАМИ ОРГАНИЗАЦИИ

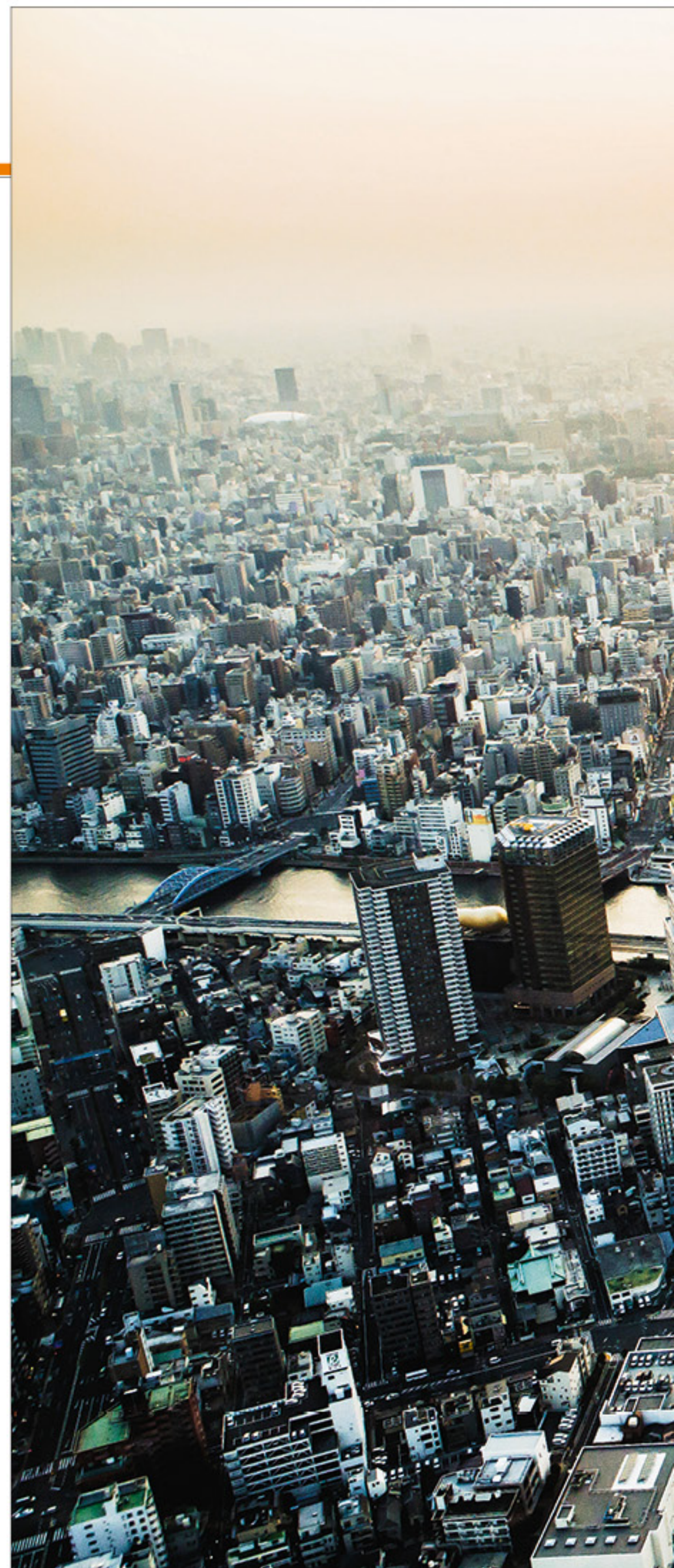
Однако та же электронная коммерция, которая развилась в цифровой бизнес, подразумевает, что автоматизированные (поддерживаемые информацией и приложениями) бизнес-процессы выходят за рамки организации и обеспечивают взаимодействие с клиентами, поставщиками, правительственными организациями и третьими сторонами. Примечательно, что и угрозы, которые раньше концентрировались вокруг информационных систем, с развитием социальных сетей и мобильного интернета приобрели совершенной иной характер. Именно изменение характера бизнеса, появление новых прямых «цифровых» каналов продаж и новых угроз для этих каналов явилось причиной качественных изменений в информационной безопасности. Что собственно и отразилось в новых терминах — Digital Security или Cybersecurity.

Это качественное изменение не произошло моментально и не во всех секторах экономики сразу. Одно можно сказать совершенно точно — финансовый сектор был в первых рядах этих изменений.

ДИКТУЕТ БИЗНЕС

Это приводит нас к первому тезису: кибербезопасность — это проблема и ответственность прежде всего бизнеса, а не ИТ. Раскроем этот тезис:

- ♦ Безопасность касается всех сотрудников.
- ♦ Безопасность выходит за пределы специфичных для ИТ процессов и технологий, от предсказуемого контекста к реакции на неизвестное (переход от ИБ-самураев к ИБ-ниндзя, по Gartner).



♦ Цифровая революция, происходящая в финансовом секторе, означает прямое взаимодействие с клиентом (прямой канал продаж). Характер такого взаимодействия определяется индивидуально для каждой группы клиентов соображениями бизнес-стратегии компании. Характер угроз ИБ, таким образом, может зависеть от решений бизнес-подразделений компании.

♦ Характер угроз, возникающих в новых каналах продаж, может не иметь никакого отношения к ИТ.



♦ ИБ может иметь собственный взгляд на вещи, который не совпадает со взглядами ИТ (например, на назначение прав доступа привилегированным пользователям).

♦ Преступные группировки осведомлены о внутреннем устройстве коммерческих², но (возможно) и центральных банков³! Это означает, что в состав пре-

ступных группировок входят действующие, либо недавно покинувшие банки сотрудники ИТ.

ДИКТУЕТ КЛИЕНТСКИЙ ОПЫТ

Второй тезис проистекает из самой природы цифрового бизнеса: клиентский опыт (ощущения клиента от взаимодействия с продавцом или сотрудника — с компанией) диктует характер многих решений, которые применяются для защиты цифровых каналов продаж. Раскроем этот тезис:

♦ ИБ должна постоянно балансировать между требованиями защиты информации и возможностью комфортно для клиента ведения бизнеса.

♦ В цифровом бизнесе огромную роль играет Digital Identity, особенно аутентификация, которая формируется под воздействием требований клиентского опыта и борьбы с мошенничеством, далеко выходящим за рамки ИТ. Дружественный, удобный и безопасный интерфейс порождает положительный клиентский опыт, да и просто гамму позитивных эмоций

² См. интервью с замначальника ГУБЗИ ЦБ А.М. Сычевым <http://www.plusworld.ru/journal/online/art197552/>

³ См. <http://blogs.wsj.com/indiarealtime/2016/05/10/fbi-suspects-insider-involvement-in-81-million-bangladesh-bank-heist/>

у клиента, что не может не сказаться на продажах.

- ♦ Изменения, которые необходимо провести в организации для реализации цифрового бизнеса, далеко выйдут за пределы ИТ.

- ♦ Современная организация утратила четкие границы. Такие технологии, как BYOD, home office, облака и соцсети размывают само понятие «контролируемой зоны», заставляя сдвигать парадигму ИБ от «100% защита внутри охраняемого периметра» (бункер) к «целостность в недружелюбной среде». Последнее означает, что ИБ должна распространять свои активности за пределы организации, занимаясь киберразведкой и проактивным анализом угроз.

МОНЕТИЗАЦИЯ УСЛУГ ИБ

Третий тезис: монетизация услуг ИБ. На американском, европейском, а также и на нашем рынке мы видим постоянное движение в сторону монетизации услуг кибербезопасности, которая становится товаром, особенно на рынке b2b. С точки зрения корпоративных бюджетов, кибербезопасность начинает переходить от источника затрат к источнику прибыли.

РЕГУЛЯТОРЫ И СТАНДАРТЫ

Четвертый тезис: требования регуляторов и стандартов. Слово «комплаенс»⁴ уже плотно вошло в жаргон специалистов в области информационной безопасности, учитывая существенные (и, порой, — заслуживающие лучшего применения) усилия правительств по контролю киберпространства. Некоторые крупные финансовые организации даже ввели должности ответственных за выполнения требований регуляторов (Chief Compliance Officer, CCO), существенную долю в работе которых занимают вопросы соответствия требованиям по безопасности персональных данных, платежной информации, ин-

⁴ COMPLAINT представляет собой соответствие какому-либо внутренним или внешним требованиям или нормам (Википедия).

Противоречия между ИТ и ИБ неизбежны в любом случае, внутри отдела или внутри одной компании. Однако, именно из противоречий рождается новое

сайдерской информации, банковской и налоговой тайны и т.д. Обратной стороной таких усилий по комплаенсу является формализация требований ИБ, вне зависимости от контекста деятельности компании и движимых этой деятельностью целей и задач ИБ. Это приводит к неэффективному использованию ресурсов подразделений ИБ на так называемую «бумажную безопасность».

С точки зрения стандартов в области информационной безопасности, таких как СТО БР ИББС и ISO 27001, разделение обязанностей и ответственности между ИТ и ИБ является рекомендуемой практикой. Например, СТО БР ИББС идет даже дальше, рекомендуя службам ИТ и ИБ иметь разных кураторов на уровне руководства организации и разные бюджеты (пункт 8.2.1 СТО БР ИББС-1.0–2014).

ЗА И ПРОТИВ

Что же плохого в том, что ИБ будет подчиняться ИТ? Безусловно, здесь есть свои положительные стороны:

- ♦ Упрощенное взаимодействие внутри организации.

- ♦ Быстрое проведение изменений — быстрый вывод продуктов и услуг на рынок (существенное конкурентное преимущество).

- ♦ Упрощенный процесс бюджетирования (безусловный плюс для любых организаций).

- ♦ Упрощенное управление людьми и компетенциями.

Однако стоит понимать, какова цена таких выгод:

- ♦ Противоречия интересов из-за разности целей ИТ и ИБ.

- ♦ Объективность оценок деятельности ИБ оказывается под вопросом: различные показатели эффективности

и разная отчетность (например, разрешение инцидентов ИТ и ИБ может измеряться совершенно по-разному).

- ♦ Взаимодействие ИТ и ИБ порождает противоречие интересов при внедрении мер ИБ. С точки зрения бизнеса или ИТ применение таких мер может замедлять реализацию ИТ-проектов или вносить ограничения в свойства реализуемых с помощью ИТ продуктов и услуг.

- ♦ Если ИБ будет подчиняться ИТ, то внедрение мер ИБ будет неизбежно иметь пониженный приоритет (со всеми вытекающими рисками для бизнеса).

- ♦ Учитывая, что ИТ становится единственным подразделением организации, имеющим компетенцию в части использования и распределения ИТ-ресурсов, управления доступом к чувствительным данным, появляется риск потери контроля за действиями ИТ со стороны топ-менеджмента организации.

- ♦ Информация о рисках ИБ может доводиться до менеджмента организации выборочно.

- ♦ Бюджет ИБ, который контролируется ИТ, означает, что для обоснования инвестиций ИБ будет просителем, который ассоциируется с противоречащими ИТ интересами. Как показывает практика, запуск проектов ИБ в такой ситуации затруднен.

Зачастую, наличие отдельного подразделения ИБ в организации позволяет разгрузить ИТ-менеджмент от чуждых им функций, таких, как контроль администраторов или комплаенс. Стоит лишь намекнуть им о том, что им более не придется разрабатывать политики и руководства безопасности, решать проблемы с соблюдением бесчисленных законов, правил и стандартов, как они становятся приверженцами разделения ИТ и ИБ.

ВЫХОД ЕСТЬ. ПРОТИВОРЕЧИЯ ОСТАЮТСЯ

Очевидный выход известен всем — это раздельное подчинение ИБ и ИТ руководству компании, когда противоречие интересов разрешается выше уровня оперативного руководства каждой из областей. (Здесь следует сделать оговорку: многое зависит от размера организаций. Для малых организаций разделение таких функций может быть затруднительно).

Противоречия между ИТ и ИБ неизбежны в любом случае, внутри отдела или внутри одной компании. Однако, именно из противоречий рождается новое. ИБ функционально тяготеет ближе к физической и экономической безопасности, в то время как ИТ — ближе к операционной деятельности.

Наладив тесные контакты с экономической безопасностью, ИБ может обогатить ИТ сервисы информацией об актуальных угрозах и мерах защиты, оценить безопасность поставщиков услуг и контрагентов, дать адекватную оценку рисков ИТ сервисов.

Несмотря на то, что в будущем роли ИТ и ИБ будут и далее разделяться,

НЕМНОГО ОПРЕДЕЛЕНИЙ

Кибербезопасность, безопасность киберпространства — сохранение конфиденциальности, целостности, доступности информации в Киберпространстве (ISO 27032 4.20).

Киберпространство — сложная среда, образующаяся в результате взаимодействия людей, компьютерных программ и сервисов в сети Интернет посредством технологических устройств и сетей, подключенных к Интернету, не существующая ни в какой физической форме (там же, 4.21).

только тесное взаимодействие ИТ и ИБ будет приносить желаемые для организации результаты — быстрый вывод прибыльных продуктов на рынок с минимальным риском.

ЗАКЛЮЧЕНИЕ. У ОДНОЙ РЕКИ

В заключение, нам бы хотелось сформулировать несколько тезисов, которые завершат эту статью:

- ♦ ИБ и ИТ дополняют, а не замещают друг друга, например, в управляющих комитетах или в реакции на инциденты.
- ♦ Внедрение Agile, который трансформирует традиционную модель разработки банковских (и прочих) продуктов,

означает более тесное взаимодействие ИТ и ИБ на уровне исполнителей.

♦ Роли типа BISO (Business Information Security Officer) и координатора ИБ внутри ИТ могут сгладить имеющиеся противоречия и упростить взаимодействие между ИБ, ИТ и бизнесом.

♦ Только вместе ИБ и ИТ смогут обеспечить выполнение политик ИБ.

♦ Подобно тому, как повышение степени разделения труда и повышение степени кооперации в производстве сложных товаров стало гигантским шагом для человечества, четкое разделение функций ИБ и ИТ и их более тесное сотрудничество принесут дальнейшие выгоды компаниям.



Александр ВЕСЕЛОВ
руководитель отдела
технического консалтинга
ООО «С-Терра СиЭсПи»

В зависимости от размера организации и зрелости её бизнес-процессов функции безопасности могут возлагаться на различные подразделения. Но противоречия между «безопасниками» и другими отделами возможны независимо от структуры, ведь многие до сих пор не осознают роль безопасности в успешном развитии компании, полагая, что безопасность — это только расходы. На самом деле это далеко не так. Прибыль от защищенности оценить непросто, но, тем не менее, вполне возможно.

Короткий пример. После технического сбоя и последовавшего за ним неприятного инцидента, связанного с безопасностью данных, заказчик решил построить собственную систему для защиты канала связи между ЦОД. Для реализации проекта было выбрано оборудование С-Терра. В итоге за год эксплуатации не случилось ни одного ИБ-происшествия, и в несколько раз снизилось количество жалоб от ИТ-отдела на скорость передачи данных. На этом примере ясно видно, что не только безопасность выросла, но и сгладились вечные противоречия между ИТ и ИБ.

А все потому, что безопасность стоит рассматривать как сервис для бизнеса, при котором залог успеха — тесное сотрудничество и понимание общих целей.

BIS-KOMМЕНТАРИЙ



Алексей БАБЕНКО
ведущий менеджер
по развитию бизнеса
компании «Информзащита»

КАК НАЙТИ ВОЛКА В ОВЕЧЬЕЙ ШКУРЕ

или Выявляем внутреннее мошенничество

Недавно поймал себя на мысли, что сообщения о мошенничестве в СМИ уже не вызывают у меня профессиональный интерес: такие случаи перестали быть единичными, СМИ то и дело публикует информацию об очередном инциденте. Интересно, что в большинстве случаев мошенниками оказываются собственные сотрудники. Исходя из моего опыта аудита банков, корпоративные меры безопасности чаще всего направлены на внешнего, неизвестного злоумышленника, а в это время инсайдер проворачивает очередную аферу.

В 2016 году компания KPMG опубликовала очередную версию исследования (Global profiles of the fraudster 2016), позволяющую взглянуть на типичный профиль мошенника.

В 79% случаев это мужчина и только в 17% — женщина (в некоторых случаях гендерных данных нет). Возраст 37% мошенников — от 36 до 45 лет, в следующий возрастной диапазон от 46 до 55 лет попадают еще 31% злоумышленников. Видно, что львиную долю потенциальных мошенников составляют

люди средних лет, при этом в самой молодой возрастной группе от 18 до 25 лет только 1% нарушителей.

65% случаев мошенничества совершается внутренними сотрудниками организаций, еще 21% — бывшими сотрудниками. Таким образом, преступники — это люди, знакомые с внутренним устройством компании. Интересно, что больше половины инсайдеров на момент совершения мошенничества работали в компании более 6 лет. Это еще одно подтверждение того, что зачастую злоумышленники хорошо знакомы со всеми тонкостями рабочего процесса и хорошо знают о возможных слабостях и недостатках защиты.

Принцип разделения обязанностей уже не является панацеей: в 62% случаев инциденты совершаются в результате сговора сотрудников. При этом каждый пятый случай произошел в результате сговора 5 и более сотрудников.

Что же дает возможность совершать злонамеренные действия? Согласно исследованиям, в большинстве случаев (61%) это недостаток внутреннего контроля, а в 44% случаев мошенни-

ки имели привилегии для осуществления действий в обход контрольных мер.

Опираясь на аналитику коллег, можно сделать вывод, что «классические» способы предотвращения мошенничества все хуже предотвращают инциденты. Проверенные сотрудники, работающие много лет, принцип разделения ответственности — все это не является надежными защитными мерами. Не стоит забывать и о среде, в рамках которой протекают бизнес-процессы. Сердце любого современного банка состоит из ИТ-систем. Это накладывает дополнительные требования к предотвращению несанкционированных действий.

Иллюстрировать свои доводы я бы хотел случаем, который освещался в СМИ. Операционист банка, используя легитимные полномочия, находил клиентов со значительными суммами на вкладах и передавал их паспортные данные сообщникам. Изготовив поддельные документы, злоумышленники шли в произвольное отделение и получали привязанную к счету клиента платежную карту, а затем снимали деньги через банкоматы.

В данном случае реализованные технические меры не предотвратили мошенничество, а действия сотрудника банка осуществлялись в рамках его служебных полномочий.

Помимо «классических» защитных мер, технических и организационных, можно выделить системы, направленные

Важно отметить, что простое внедрение антифрод-системы не всегда усложнит мошенникам жизнь. Важно сформировать правильные процессы анализа и расследования выявленных инцидентов



ные на противодействие мошенничеству. Если стандартные средства контроля призваны не допустить совершения несанкционированных манипуляций, то антифрод-системы изначально оценивают весь входящий поток операций как потенциально мошеннические. Таким образом, даже используя легитимные меры обхода контрольных мер (например, в результате сговора или с использованием служебных привилегий), мошеннические операции все равно будут выявлены из общего объема.

К основным способам выявления мошенничества относят два вида: сценарные и статистические. При сценарном анализе контролируется заведомо известное поведение нарушителя: перевод денег на подложные счета, выполнение операций от имени клиента, изменение критичных параметров, нарушение хода процесса и обход части контрольных процедур. Плюсами сценарных правил является высокая точность работы, возможность использования скоринговой модели (когда каждое действие по отдельности не кажется подозрительным, но вместе представляет угрозу) и простота реализации. Недостаток такого анализа состоит в необходимости задавать заранее известные сценарии. Понятно, что создать стопроцентное покрытие — задача невыполнимая.

Решить проблему сценарного анализа призваны статистические правила. В них, на основании исторических данных, формируется стандартный профиль для различного вида сущностей (сотрудников, счетов, банковских продуктов, клиентов). Далее каждое действие оценивается с позиции отклонения от значений стандартного профиля, и если отклонения оказываются больше доверительных интервалов, то правило сообщает о выявлении подозрительной операции. Величина доверительного интервала может быть пе-

ременной величиной и высчитываться автоматически, исходя из совершаемых действий, результатов срабатывания правил и расследований результатов срабатываний.

Вернемся к примеру с незаконным хищением денег при содействии сотрудника банка. Система противодействия мошенничеству сразу могла бы выявить следующие аномалии: подозрительный поиск сотрудником счетов со значительными суммами, перебор клиентов; нетипичный для клиента запрос на выпуск платежной карты (например, при наличии действующей аналогичной карты); нетипичный способ вывода денег со вклада; использование новой карты для снятия большой суммы. Таким образом, предотвратить мошенничество можно было на каждом из его этапов.

Важно отметить, что простое внедрение антифрод-системы не всегда усложнит мошенникам жизнь. Важно сформировать правильные процессы анализа и расследования выявленных инцидентов. На первых этапах формирования правил система будет генерировать большое количество ложных срабатываний, которые должны быть отработаны, а соответствующие уточнения внесены в правила. Новые и потенциально возможные инциденты должны постоянно анализироваться и служить входной информацией для формирования новых правил.

В случае с внутренним мошенничеством, отдельная задача состоит в том, чтобы сформировать правильные процедуры реагирования. Если вы спросите у потенциального мошенника, он ли совершил злодеяние, то он вряд ли ответит в утвердительной форме. Если в случае с кражей клиентских данных извне подтвердить подлинность операции можно у клиента, то при действиях инсайдеров это не всегда возможно.

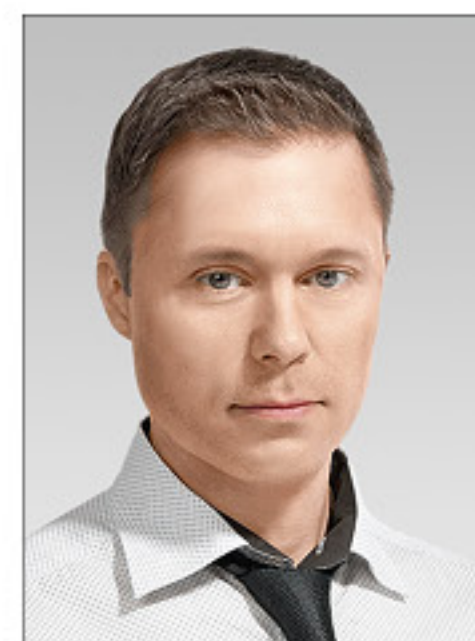
При проведении расследования нужно выбрать и придерживаться стратегии, при которой изначально собирается доказательная база и информация об инциденте, а далее производится разбирательство с сотрудником. Конечно, при этом нужно учитывать крайние ситуации, когда расследование проводить уже поздно, да и сам сотрудник больше никогда не попадетс вам на глаза. В случае опасности проведения необратимых действий, необходимо оперативное пресечение и инициация расследования постфактум проведенных операций. Для таких ситуаций минимальным реагированием должно стать взятие нерадивого сотрудника «на карандаш» и пристальное внимание к его действиям в рамках выполнения своих рабочих обязанностей. В системе противодействия мошенничеству для таких сотрудников должны быть скорректированы значения коэффициентов критичности срабатывания правил.

* * *

Проблема внутреннего фрода — обширная тема, которой можно заниматься в рамках практически каждого из банковских процессов. Разумным в данном случае выглядит подход покрытия наиболее критичных областей: платежных процессов, операций с ценными бумагами, кредитные операции. В дальнейшем, на основе выстроенной системы и процессов противодействия мошенничеству, подключать новые области. Альтернативным вариантом может стать отрицание банком проблемы мошенничества как таковой и учет возможных убытков в операционные расходы. Этот подход имеет право на существование, каждый банк сам определяет для себя допустимые риски и величину возможных издержек, которую он готов заплатить. Однако, случаи, когда результат мошенничества начинает влиять на жизнеспособность всего банка, уже встречаются, и такие риски игнорировать нельзя.

ТЕЧЁТ!

Пять явных признаков утечки информации в организации



Денис СУХОВЕЙ
директор департамента развития
технологий компании «Аладдин Р.Д.»

В наши дни бизнес большинства организаций сопровождается поддержкой сложных ИТ-систем и централизованных хранилищ, в которых так или иначе уже реализована защита информации. Работа с файлами, находящимися в хранилище, нередко бывает неудобной, поэтому пользователи часто копируют файлы из ИТ-систем и хранилищ, себе на рабочую станцию или внешний носитель. При этом скопированные данные хранятся в незащищённом незашифрованном виде. Эти действия часто обосновываются скоростью доступа/обработки, удобством, необходимостью работы вне офиса, командировками и т.п., сопровождаясь фразой типа «Так проще и удобнее».

Ложное ощущение защищённости создают обычно применяемые меры безопасности централизованных систем, ведь на первый взгляд доступ к носителям информации на рабочих станциях и ноутбуках могут получить только доверенные люди, однако в реальности дела обстоят совсем не так. Доступ к информации на дисках рабочих станций, серверов или ноутбуков может осуществляться в следующих ситуациях:

- ♦ работы администратора по настройке или обслуживанию компьютерной техники;
- ♦ утеря ноутбука, на котором хранится и обрабатывается критичная информация;

- ♦ транспортировка внешних носителей с незащищённой критичной информацией;

- ♦ ремонт компьютерной техники с вывозом из офиса в сервисный центр;

- ♦ изъятие компьютерного оборудования по судебным решениям или без них;

- ♦ переезд и перевозка компьютерной техники в другое помещение или новый офис;

- ♦ утилизация устаревшего, вышедшего из строя компьютерного оборудования.

Получить доступ к незащищённым данным в таких ситуациях достаточно легко, но обнаружить утечку данных вследствие них весьма затруднительно. Например, при отсылке «намертво» зависшего компьютера на ремонт в сервисный центр возникает существенный риск несанкционированного доступа к конфиденциальной информации. Такая утечка информации может никогда и не обнаружиться. Ещё одно распространённое заблуждение — на ноутбуках хранится информация, потеря которой не может причинить вред компании, ведь копии файлов есть в централизованном файловом хранилище. Для того, чтобы опровергнуть это суждение, достаточно представить себе возможные последствия утечки информации с потерянного ноутбука генерального директора компании:

- ♦ информация о финансовом положении дел организации;

- ♦ персональные данные сотрудников;

- ♦ переписка с клиентами и другие критичные данные систем CRM- и ERP-систем;

- ♦ стратегические планы организации, анализ рынка и конкурентной среды и т.п.

По мнению специалистов компании «Аладдин Р.Д.», существуют совершенно конкретные признаки и ситуации, которые явно свидетельствуют о наличии потенциальных проблем утечки конфиденциальной информации в организации.

Если в компании обнаруживается один или несколько из нижеперечисленных признаков, то риски утечки важной или конфиденциальной информации существенно возрастают. Это обстоятельство должно послужить определённым «звонок» для службы информационной безопасности. Безусловно, традиционным методом решения подобных потенциальных проблем является мониторинг утечек информации посредством системы DLP (Data Leak Prevention). Однако, подобные системы требуют внушительных финансовых затрат на их внедрение и дальнейшее сопровождение. Альтернативным подходом к решению подобных проблем является применение средств шифрования информации на дисках серверов и рабочих станций. Самые важные и наиболее критичные из них перечислены ниже.

1. «Текучка» — ротация персонала, организационные изменения или массовые увольнения (сокращения) сотрудников. Кризис и сложные экономические условия заставляют руководство большинства компаний идти на решительные меры в отношении штата сотрудников. В таких условиях вероятность потенциальной утечки значительно возрастает. Потенциальная опасность исходит не только от «пострадавших» сотрудников. Обычно массовые увольнения или изменения в организационно-штатной структуре организации снижают общий уровень мотивации персонала. «Обиженный» сотрудник, наделённый доступом к конфиденциальной, критичной или служебной информации, является слабым звеном в общей системе безопасности. Статистически наиболее часто совершаемые нарушения информационной безопасности у таких сотрудников — кража и передача информации третьим лицам. Функции шифрования информации на диске и контроль копирования защищаемой информации на USB-устройство, реализованные в системе Secret Disk Enterprise, позволят существенно снизить риски утечки при интенсивной ротации кадров в организации.

2. Командировки — рабочий распорядок сотрудников организации предполагает большое количество деловых встреч/поездов/командировок. Современный «мобильный» сотрудник, выезжающий за пределы офиса в локальную или дальнюю командировку, оснащён целым рядом электронных средств коммуникации. Однако наиболее востребованным инструментом в такой ситуации является ноутбук. Подавляющее большинство ноутбуков, вывозимых в командировку, содержат служебную информацию, коммерческую тайну, конфиденциальную информацию. По статистике утечек, ноутбук, утерянный или украденный в общественном месте, является причиной № 1 в утечке ценной информации. Функции шифрования системного раздела жёсткого диска и шифрования дополнительных разделов, реализованных в системе Secret Disk Enterprise, позволят исключить возможность доступа к данным на потерянном или украденном ноутбуке.

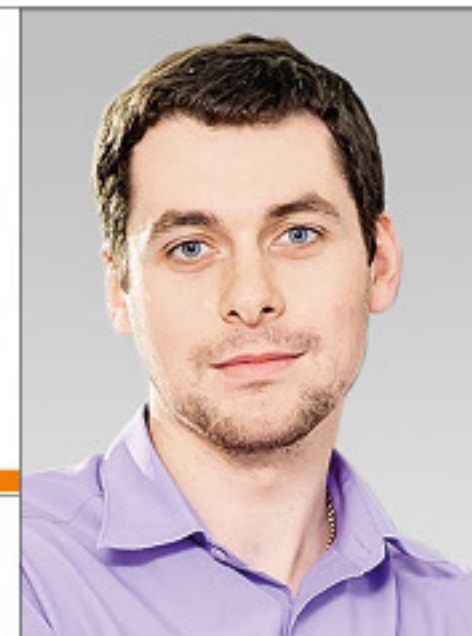
3. Работа с контрагентами или филиалами — регулярный внешний обмен важной и конфиденциальной информацией. Некоторые производственные процессы в организации построены на основе обмена информацией с внешними контрагентами. Зачастую такому обмену подлежит служебная и конфиденциальная информация. Информацию передают на разнообразных флеш-носителях и т.п. В ходе транспортировки такая информация зачастую теряется или даже намеренно изменяется. Доступ к такой информации не контролируется службой безопасности. Такой вид обмена существенно повышает риски утечки важной информации. Функции использования криптоконтейнеров и шифрования виртуальных внешних USB-дисков, реализованные в системе Secret Disk Enterprise, позволят надёжно защитить передаваемые третьим лицам данные.

4. Сложная ИТ-инфраструктура и несколько ИТ-администраторов. Сложность инфраструктуры и информационных систем — это очень важный осложняющий фактор для службы информационной безопасности. Такие инфраструктуры зачастую обслуживаются несколькими администраторами, имеющими равные, максимальные права доступа к серверам и рабочим станциям организации. Соответственно, возможность неконтролируемого доступа к конфиденциальной информации свидетельствует о наличии потенциальных возможностей утечек критичной и важной информации. Это обстоятельство осложняется традиционно непростыми отношениями руководства организации с ИТ-администраторами. Очевидно, что демотивированный или «обиженный» сотрудник с правами привилегированного пользователя — это бомба замедленного действия. О масштабах последствий утечки критичной информации в данном случае можно только догадываться. Функции использования шифрования папок в системе Secret Disk Enterprise позволят «изолировать» системного администратора, не нарушая при этом бизнес-процесс администрирования защищаемой системы.

5. Мобильный офис — большой парк ноутбуков, используемых в компании. У 45% заказчиков доля ноутбуков, используемых в современных компаниях, достигает 45% от общего числа компьютерной техники. Ноутбуки — это удобно и эффективно. Однако, современный ноутбук является замкнутой аппаратной средой, находящейся на гарантии фирмы-производителя. Сотрудники ИТ-служб в компаниях не имеют возможности ремонта и даже диагностики проблем неработоспособности ноутбука. При поломке, сбоях в работе и т.п. ноутбуки передаются в сервисный центр (по гарантии). Вместе с ноутбуком в сервисный центр вынужденно передаётся вся конфиденциальная информация, находящаяся у него «на борту». Таким образом, ни служба безопасности, ни ИТ-служба компании не могут контролировать доступ работников сервисных центров к информации, находящейся на диске переданного ноутбука. Очевидно, что данное обстоятельство является высоко-критичной проблемой утечек важной и конфиденциальной информации. Зашифрованная системой Secret Disk Enterprise информация будет недоступна для сотрудников сервисного центра, даже если при передаче ноутбук «намертво» завис, данные на диске останутся зашифрованными.

* * *

Шифрование данных является единственным разумным способом предотвращения утечек данных с потерянных ноутбуков, мобильных компьютеров и внешних носителей информации. Однако шифровать требуется не только «мобильную» информацию, стационарные рабочие станции и файловые сервера компании также попадают в группу риска утечек важной или критичной для бизнеса информации. Обладая гибкостью функционала шифрования и позволяя службе безопасности обеспечивать криптографическую защиту целого парка компьютерной техники в современном офисе, система прозрачного шифрования Secret Disk Enterprise является идеальным выбором, совмещающим надёжность, простоту и экономичность.



С SIEM`ОМ ИЛИ НА ЩИТЕ: БАНКОВСКАЯ СПЕЦИФИКА

За последние 1,5–2 года кибератаки на банки из единичных случаев стремительно превращаются в эпидемию. При этом средний срок обнаружения атаки составляет 188 дней. Максимальный срок присутствия злоумышленника в инфраструктуре с момента взлома до его обнаружения, зафиксированный нашими экспертами, — 7 лет. А всего лишь через 1–2 недели после проникновения найти все скомпрометированные системы почти невозможно: злоумышленник получает возможность использовать легальные учетные записи и встроенные утилиты администрирования и пр. То есть разрыв между датами компрометации инфраструктуры и обнаружения атаки недопустимо велик.

Ключевым средством выявления сложных атак и инцидентов ИБ могло бы стать решение класса Security Information and Event Management (SIEM). Тем более, что в большинстве организаций проекты по внедрению SIEM-систем уже были выполнены. Но статистика успешных атак говорит, что что-то все же не сработало...

ЦЕЛЬ ТАМ, ГДЕ ДЕНЬГИ

Банковский сектор относится к числу тех отраслей, где монетизация кибератак — относительно понятная для злоумышленников задача. Поэтому киберпреступность проявляет к ним особенно пристальный интерес: только за полгода (с октября 2015 по март 2016 года) FinCERT зафиксировал более 20 атак. При этом банки спасли только 1,6 из 2,87 млрд руб. У всех на слуху история банка «Кузнецкий», чей ущерб в результате атаки составил око-

ло 470 млн рублей, или «Металлинвест-банка» (со счетов которого похищено 200 млн руб.), «Таатта» (потерявшего 100 млн руб.), «Русского Международного банка» (похищено 500 млн руб.) и др. Как видим, разговор идет об ущербе, исчисляющемся сотнями миллионов. И это еще без затрат на восстановление скомпрометированной инфраструктуры, которые также могут быть сопоставимы со стоимостью разворачивания инфраструктуры с нуля.

Схема краж была такова: по e-mail отправлялось «невидимое» для антивирусов вредоносное ПО. Далее с помощью SMB-запросов сканировалась локальная сеть для заражения других машин, на которые потом загружался ботнет-клиент с функцией удаленного управления. Что можно противопоставить такой атаке? Система класса SIEM, например, может отметить факт получения сотрудниками одинаковых вложений и если с их ПК одновременно начнут уходить SMB-запросы, то это вызовет подозрения. Сопоставление таких активностей могло бы помочь детектировать атаку. Хотя можно подождать и загрузки ботов на зараженные ПК: то, что с нескольких компьютеров по HTTP ушли одинаковые запросы,

а содержимое веб-страницы, куда заходили боты, нехарактерно для конкретного человека — сигнал для поднятия тревоги. Например, взломав банк «Кузнецкий», злоумышленники от имени сотрудника, ответственного за отмену транзакций, в автоматическом режиме отменили около 3000 операций. А это редкая и не простая операция и не может выполняться ежесекундно. Даже если SIEM-система пропустила бы все шаги злоумышленников при входе в инфраструктуру, то число операций по отмене транзакции — явно аномально. И сигнал тревоги поступил бы уже после первых из них.

Для идентификации подобных событий необходимы системы обнаружения (IDS или средства анализа трафика), но только SIEM на ранней стадии сможет связать все события в единую цепочку.

ПОЧЕМУ ЖЕ ВСЕ ТАК ПЛОХО?

Итак, практика показывает, что, хотя SIEM-системы и используются большинством компаний, удручающая статистика по скорости выявления атак сохраняется. В чем дело? Причин этому несколько. Во-первых, целенаправленные атаки (APT) выявляются толь-

В среднем за два года инфраструктура компании меняется на 80%. Поэтому типичный SIEM часто напоминает автомобиль, половину времени простаивающий в сервисе: его надо постоянно «дотюнивать» вслед за конфигурационными изменениями в ИТ-инфраструктурах. И если вы не занимались постоянной адаптацией системы, то уже через 2–3 года ваш автомобиль марки SIEM полностью съедет на обочину: он, конечно, еще помагает габаритами, но обеспечивать покрытие всех систем и сбор актуальных данных — не сможет.



ко через множество разрозненных некритичных событий, выстраиваемых в цепочку. А в случае с типичными SIEM-системами ее нужно выстраивать для каждой отдельной системы и инфраструктуры. Это колоссальные затраты на создание и поддержку правил в актуальном состоянии.

Во-вторых, стоит отметить сложность и трудозатратность внедрения: нужны интеграция и обеспечение взаимодействия SIEM со множеством систем. И невозможно выполнить все работы разово — это процесс: конфигурационные изменения различного характера в ИТ-инфраструктурах крупных компаний происходят практически ежедневно. И именно в необходимости постоянной доработки SIEM-систем (особенно, если для этого требуется привлечение интегратора и запуск нового интеграционного проекта) кроется одна из причин того, почему после внедрения они просто «кладутся на полку».

Работа системы основана на логменеджменте — сборе данных обо всем, что происходит в рамках инфраструктуры (с каких-то систем ИБ, коммутационного оборудования, операционных систем, бизнес-приложений, в том числе и собственной разработки). Поэтому нельзя обойти вниманием вопрос подключения источников информации, а их число может исчисляться десятками. Этот длительный и крайне трудозатратный процесс. Практически ни одна SIEM-система не покрывает все необходимые источники «из коробки». И это тоже одна из причин их слабой эффективности. Подключение всех

существующих источников в рамках проекта внедрения, равно как и подключение новых в ходе последующей технической поддержки, без переключения этих задач на заказчика или интегратора — уникальная для нашего рынка ситуация.

ЭКСПЕРТИЗА И ЗНАНИЕ ИНФРАСТРУКТУРЫ

MaxPatrol SIEM «понимает» любую инфраструктуру, автоматически подстраиваясь под все изменения: все имеющиеся и получаемые данные — конфигурация узла и его настройки, установленное ПО, сетевая активность, логи — унифицируются и выстраиваются вокруг каждого из активов с учетом их расположения и взаимосвязей (актив — любой элемент инфраструктуры, сетевой узел, идентифицируемый по различным признакам). Она постоянно обогащается данными из новых событий, сканирований, сетевого трафика и от агентов на конечных точках. За счет этого в MaxPatrol SIEM выстраивается актуальная в любой момент времени виртуальная модель инфраструктуры предприятия. И все эти данные используются в правилах корреляции.

В одной из компаний с помощью MaxPatrol SIEM была обнаружена деятельность ряда АРТ-групп посредством анализа различных событий из логов антивирусов. Есть в копилке системы и опыт выявления квалифицированных внутренних мошенников на основе анализа сетевого взаимодействия между подразделениями компании.

Также концепция MaxPatrol SIEM предусматривает возможность передачи экспертизы заказчику, для чего мы внедряем базу знаний Positive Technologies Knowledge Base (РТКВ). Это высокоуровневый, постоянно актуализируемый набор данных, основанный на нашем 15-летнем опыте проведения тестов на проникновение и аудитов защищенности. В результате система сможет обновлять данные об известных моделях атак и паттернах поведения хакеров, учитывать новые уязвимости и эксплойты, автоматически изменять правила корреляции, которые накладываются на инфраструктуру заказчика, не требуя ручной настройки.

В итоге для эффективной эксплуатации SIEM компании не всегда необходима обширная команда аналитиков: управление из единого интерфейса позволяет решать типовые задачи силами даже одного эксперта. Что существенно упрощает работу с системой.

* * *

Таким образом, для эффективного выявления инцидентов ИБ нужна не SIEM-система с классическим набором функциональных возможностей, а экосистема из множества решений, обеспечивающая понимание актуальной модели инфраструктуры на любой момент времени, а также привносящая в продукт практическую экспертизу нашего исследовательского центра. При правильной настройке она дополняет антифрод-решения и сможет в прямом смысле слова спасать деньги и репутацию кредитной организации.



СКАЗКИ-ПОДСКАЗКИ ОТ С-ТЕРРА

Жил-был царь. Так начинается множество сказок. Но наши безопасные сказки начинаются совсем по-другому. И морали в них нет, зато есть подсказки, вернее, ПодСказки. А вот конец у наших сказок традиционный — всегда счастливый!

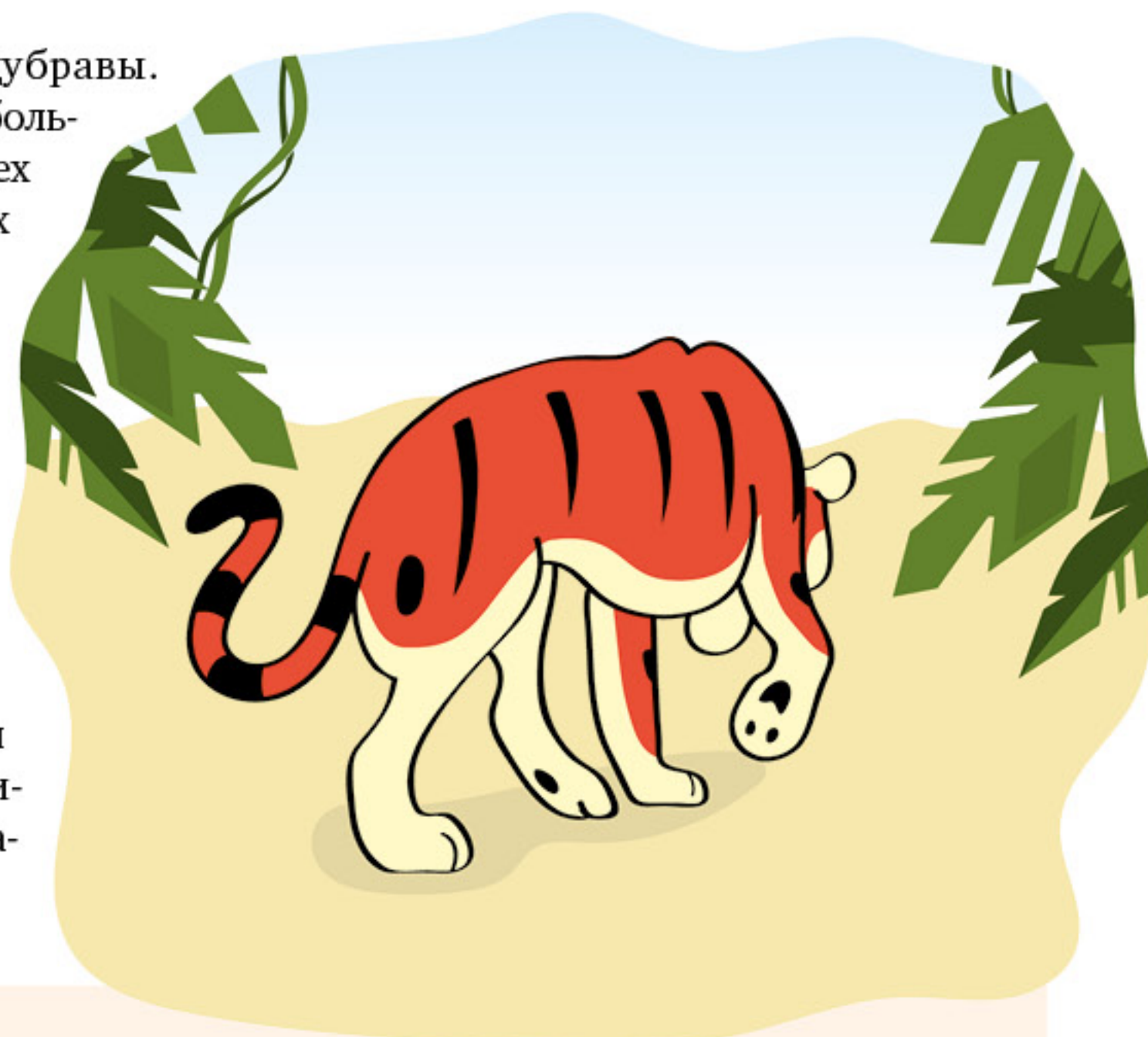
СКАЗКА ПЕРВАЯ. ПРО МЕДВЕДЯ И ТАЙНЫЕ ТРОПЫ

Жил-был Медведь. Берлога его находилась в самом сердце дубравы. Это была не просто берлога, а современное просторное жилище большого и серьезного правителя леса. Туда приходили известия со всех концов его вотчины, из берлог его собратьев-медведей, из заячьих и кроличьих нор, из беличьих и птичьих гнезд... Медведь правил грамотно, шустрые гонцы несли обратно в норы, гнезда, берлоги точные и толковые указы. И всё было мирно в царстве зверей, пока не повадился охотиться на гонцов ловкий и изобретательный Тигр. Хищник не просто добывал себе пропитание, а стремился захватить власть в лесу, узнать все тайны и вывести все знания. Жители леса испугались и пошли к Медведю — держать совет и искать решение.

Правитель леса не стал сомневаться. Он позвал войско лесных охотников — волков и лис — во главе с самым мудрым Лисом. Был у них давний договор, что волки и лисы не покушаются на вестников Медведя, а защищают их. Пришли охотники на общее собрание, выслушали всех, посоветовались и предложили такой план.

Вокруг берлоги Медведя сделать непролазную живую изгородь из колючих кустов, оставив для гонцов широкий проход, закрывающийся большими двустворчатыми воротами с могучими засовами и замками. Каждого гонца снабдить специальным ключом, отпирающим эти засовы и замки. Подобные надежные ограждения сделать вокруг жилища каждого лесного обитателя. А между воротами, в самых густых зарослях и лесных чащах, проложить тайные тропы, которые ни один Тигр не отыщет.

Так и сделали звери. Конечно, пришлось потрудиться, зато снова настала мирная и счастливая жизнь в лесу — ушел Тигр, поняв, что попытки его безуспешны.



Дано

Банк + 20 филиалов.
Связь – по сети Интернет.
Канал в банке 100 Мбит/с,
в филиалах – по 10 Мбит/с.

Требуется

Защита по классу КС 1

Результат

Построена защищенная распределенная корпоративная сеть Банка. Защиту обеспечивают сертифицированные VPN-продукты С-Терра в соответствии с требованиями ГОСТ, на базе протоколов IPsec.

Решение

Банк – устанавливаем:

- 2 × С-Терра Шлюз 1000 (до 90 Мбит/с на IMIX и до 50 туннелей) или 2 × С-Терра Виртуальный Шлюз
- 1 × систему управления С-Терра КП на 100 лицензий

Филиалы – устанавливаем:

- В каждый по одному С-Терра Шлюз 100 (до 30 Мбит/с на IMIX и до 10 туннелей)

ПодСказка 1. Современным языком цифр

СКАЗКА ВТОРАЯ. ПРО ДАЛЬНИЕ ДАЛИ И БЕЛЫХ МЕДВЕДЕЙ

Жил-был Медведь. Жил он далеко-далеко на севере, среди льдов и полярных сияний. Вы уже догадались, что он был Белый. Конечно, там водились и другие белые медведи, но они очень редко собирались вместе — слишком далеко друг от друга жили. Как-то дошла до них весть о том, что сильно южнее, там, где густые леса и яркое солнце, живут их родственники, бурые медведи. И один из них, самый большой Медведь, правит всем лесом. И вот, на общем собрании решили белые медведи написать письмо своим лесным братьям, узнать подробнее, как они живут, как их лесное государство устроено, какие порядки установлены. Сказано — сделано. Написали они послание и отправили его со стаей Больших Птиц, которые умели летать на юг.

Скоро ли, нет ли, но те же Птицы принесли Белому Медведю ответ. В письме рассказывал Бурый Медведь о лесных обитателях, о правилах мирной жизни, о своем житье-бытье. Описывал и систему безопасного общения, которую они наладили. А еще предлагал сделать переписку регулярной, обмениваться полезными сведениями, да не с одним только Белым Медведем, а со всеми его собратьями — ведь у каждого были знания, которыми стоит поделиться, и каждому из них было интересно узнавать про жизнь в теплых краях.

В то же время, Бурый Медведь предупреждал о хищниках, которые встречаются на пути к его берлоге и просил защитить чудесных Больших Птиц и ценные послания.

Не растерялись белые медведи, сделали легкий, крепкий и надежный футляр, который можно открыть, только зная особый секретный ключ. Туда и поместили документ. Нужно сказать, что ключ этот известен всем медведям, но только им. Даже Большие Птицы эту тайну не знают, они лишь доставляют послание в футляре через большие ворота неприступной ограды вокруг берлоги Бурого Медведя.

С тех пор переписываются медведи северные и южные, делятся между собой знаниями, обсуждают события. Вот только никому не известно, о чем именно они беседуют — секрет-то медвежий.

БУРЫЙ МЕДВЕДЬ ПРЕДУПРЕЖДАЛ О ХИЩНИКАХ, КОТОРЫЕ ВСТРЕЧАЮТСЯ НА ПУТИ К ЕГО БЕРЛОГЕ



Дано

Банк и 50 удаленно работающих сотрудников.
Связь – по сети Интернет.
Канал в банке 100 Мбит/с.
Мобильные устройства:
40 – планшеты на Windows
10 – планшеты на Android

Требуется

Защита по классу КС 1

Результат

Организован защищенный доступ удаленных пользователей в корпоративную сеть Банка.
Защиту обеспечивают сертифицированные VPN-продукты C-Terra в соответствии с требованиями ГОСТ, на базе протоколов IPsec.

Решение

Банк – устанавливаем:

- 2 × C-Terra Шлюз 1000 (до 90 Мбит/с на IMIX и до 50 туннелей) или
- 2 × C-Terra Виртуальный Шлюз
- 1 × систему управления C-Terra КП на 100 лицензий

Устройства удаленных сотрудников – устанавливаем:

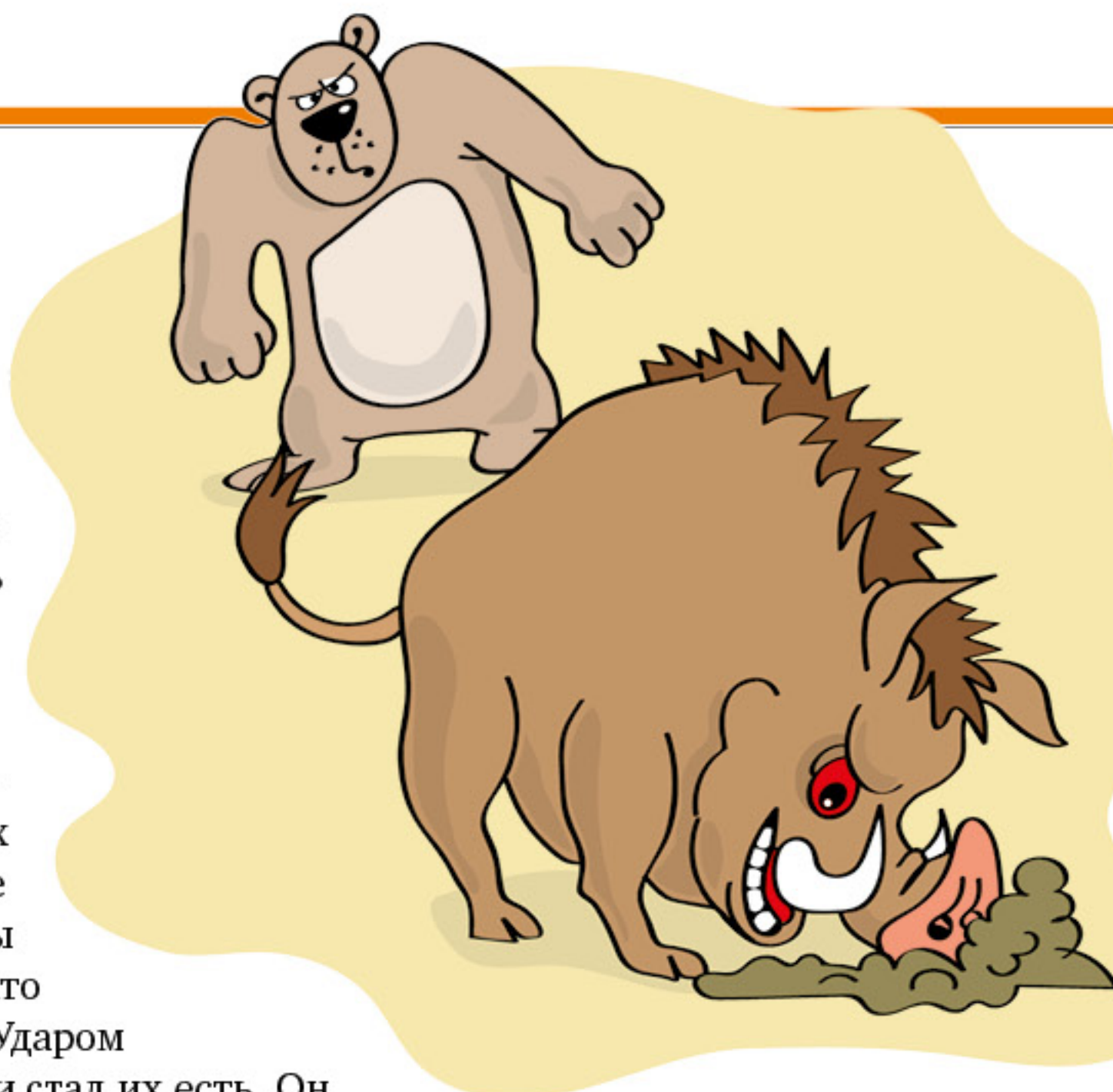
- 40 × C-Terra Клиент
- 10 × C-Terra Клиент-М

СКАЗКА ТРЕТЬЯ. ПРО КАБАНА И БОГАТСТВО

Жил-был Кабан. Большой, жирный и ленивый Кабан. Но он очень хотел разбогатеть и стать главным в лесу. Решил Кабан, что если он проберется в берлогу Медведя и украдет Главный Секрет, то станет всемогущим. А там и богатство как-нибудь образуется. Преодолея Кабан свою лень и стал рыть подземный ход. Много земли пришлось перекопать, но, в конце концов, он добрался до берлоги. Увидел там Кабан большие коробки с бумагами — все письма от Белых Медведей, записки от друзей, доклады от жителей леса Медведь хранил в огромных сундуках в дальней комнате своего жилища. Читать Кабан не умел, да если бы и мог, то это не помогло бы ему — все тексты были написаны особым способом, с секретом. Решил Кабан, что в самом большом коробе и хранится самый Главный Секрет. Ударом копыта проломил он стенку сундука, достал оттуда бумаги, и стал их есть. Он полагал, что именно так секреты и передаются. За этим неприглядным занятием Медведь и застал Кабана. Так бесславно закончились попытки Кабана получить власть и богатство.

А Медведь задумался. Понял он, что многие знания, получаемые и хранимые им, нужно поместить в более защищенное хранилище. Причем, самые важные из них нужно разделить и хранить в разных местах — чтобы в случае неприятности хотя бы часть уцелела. Оба хранилища необходимо надежно защитить от кабанов и им подобных злодеев: сделать основание из бревен, поставить крепкую изгородь, установить надежные ворота. Между хранилищами проложить широкую и удобную тайную тропу — чтобы быстро большой воз с документами можно было доставить. Для верности, вообще можно подземный туннель прокопать. А от ворот, ведущих к берлоге Медведя, до ворот хранилища организовать отдельную, очень секретную дорогу через самые непроходимые дебри.

Так и сделали звери. Хранилища получились — загляденье! Просторные, крепкие, несокрушимые. А главное — хорошо защищенные. С тех времен зажили Медведь и звери в лесу спокойно, мирно и благополучно.



Дано

Банк
ЦОД основной
ЦОД резервный
Связь – по сети Интернет
Канал в банке 100 Мбит/с.
Канал между ЦОД – 10 Гбит/с

Требуется

Защита по классу КС 1

Решение

Банк – устанавливаем:
– 2 x C-Терра Шлюз 7000 (до 2000 Мбит/с на IMIX и неограниченное количество туннелей)
ЦОД основной – устанавливаем:
– 2 x C-Терра Шлюз 7000
– 2 x C-Терра Шлюз 10G (до 10 Гбит/с на IMIX и неограниченное количество туннелей)
ЦОД резервный – устанавливаем:
– 2 x C-Терра Шлюз 10G

Результат

Организовано защищенное взаимодействие между основным и резервным ЦОДами, а также доступ по защищенному каналу к основному ЦОД из Банка.
Защиту обеспечивают сертифицированные VPN-продукты C-Терра в соответствии с требованиями ГОСТ, на базе протоколов IPsec.

ПодСказка 3. Современным языком цифр

ЭПИЛОГ

Так и в настоящей жизни: только надежная защита данных позволяет избежать затрат по их восстановлению, компенсации возможного ущерба и восполнению репутационных потерь. А обеспечить безопасность информации при передаче ее по открытым каналам оптимальным образом лучше всего с помощью решений C-Терра.



**BIS
JOB**

Интернет-портал
Образование и карьера

Миссия портала:

Информационно-аналитическая поддержка непрерывного образования как важнейшего фактора кадрового обеспечения сферы информационной безопасности России

bisjob.ib-bank.ru



Андрей КУРИЛО
доцент Финансового университета
при Правительстве Российской
Федерации, председатель Комитета
по информационной безопасности
НП НСФР, кандидат технических наук

ОБОСТРЕНИЕ ПРАКТИКОЙ

Заметки на полях РКИ-форума

И снова, 14–16 сентября 2016 года, уже в который раз в Санкт-Петербурге состоялся РКИ-форум. Так сложилось, что в его работе традиционно принимают участие разработчики средств электронной подписи, представители государственных регуляторов, работники удостоверяющих центров, юристы — специалисты в области информационного права, руководители крупных государственных структур, а также зарубежные коллеги, прекрасно владеющие самой последней информацией и нормативными актами Европейского Союза в сфере электронной подписи и электронного документооборота. Интересные доклады и возникающие дискуссии придают этому мероприятию какой-то особый, одновременно и деловой и творческий дух.



Олег Пак, Статс-секретарь-заместитель Министра связи и массовых коммуникаций Российской Федерации вручает диплом РКІ-Форума Яне Кримпе, учредителю компании B.EST Solutions



Роман Кузнецов, директор Правового департамента Минкомсвязи России

ДОСТОЯНИЕ МАСС

Смею предположить, что в значительной степени это связано с тем, что тематика электронной подписи (ЭП) + РКІ + электронный документооборот вышла из стадии формирования и начинает применяться на практике. Сейчас это уже происходит широко, с вовлечением в нее миллионов организаций и десятков миллионов наших граждан. Более того, на повестку дня начинают выдвигаться новые, без преувеличения глобальные проекты, требующие решения концептуальных, законодательных, технических и технологических задач и проблем.

Все это дает неоценимый опыт практического внедрения новых технологий электронного документооборота и безопасности, а заодно позволяет увидеть, как реализуются в жизни те концепции по использованию средств обеспечения конфиденциальности и доверия к электронному документообороту, которые были сформированы, заложены в законодательство и нормативную базу 5–10 лет назад. В свою очередь, анализ этого опыта предоставляет уникальную возможность откорректировать ранее выбранные концепции и тем самым более эффективным образом приблизиться к реализации задачи создания в стране успешно действующего «электронного правительства», улучшения взаимодействия граждан и государства, создания инфраструктуры «доверия» на национальном и транснациональном уровне.

Так как основным инструментом обеспечения доверия к электронному взаимодействию является электронная подпись, достаточно обстоятельно обеспеченная в настоящее время

законодательной и нормативной поддержкой и практически используемая уже в массовом порядке, то и выступающие в своих докладах так или иначе касались практики использования как самой электронной подписи, так и различных механизмов обеспечения доверия к ней.

Важно отметить, что вопрос доверия постепенно начинает формулироваться не только как организационно-техническая задача обеспечения доверия к работе самих механизмов электронной подписи или идентификации, а как правовой вопрос обеспечения доверия к документу как основному элементу гражданского права, как к необходимому условию реализации и обеспечения прав, порождаемых или фиксируемых документом вне зависимости от формы его представления.

Если под этим углом зрения рассматривать доклады, выступления и дискуссии, состоявшиеся на форуме, то можно выделить следующие темы, привлекавшие наибольший интерес слушателей.

ОТ СЕГМЕНТА ДОВЕРИЯ

1. Деятельность удостоверяющих центров. Либертарианская правовая концепция, положенная в основу процедур по предоставлению аккредитации удостоверяющим центрам при выполнении ими достаточно простых требований, установленных регулято-

ром, привела к возникновению целой подотрасли УЦ, разросшейся до масштабов среднего республиканского министерства времен СССР — свыше 400 отдельных юридических лиц. Есть еще филиалы и доверенные агенты, на которые предполагается возложить ответственность по выдаче сертификатов гражданам и юридическим лицам (отметим, что именно при выдаче квалифицированных сертификатов в конце прошлого года были совершены махинации, стоившие добропорядочным гражданам потери дорогой квартиры и головной боли по ее возвращению обратно в свою собственность). Для сравнения — в США, известных своими либеральными свободами в части предпринимательства, таковых только 3, а в Польше — целых 5, правда только один из них выдает квалифицированные сертификаты, а остальные — нет. И справляются.

Ответственность за выдачу гражданам и юридическим лицам квалифицированного сертификата, обладающего признаками документа, удостоверяющего личность (паспорта) и нотариально оформленной доверенности обеспечивается, в соответствии с со сложившейся практикой, только уставным фондом удостоверяющего центра и его административной ответственностью, при полном отсутствии какой-либо адекватной ответственности у персонала, собствен-

Тематика электронной подписи (ЭП) + РКІ + электронный документооборот вышла из стадии формирования и начинает применяться на практике

но и совершающего эти операции. Напомним, что нотариус, выдающий сходные по правовой силе документы, в соответствии с законом отвечает за совершаемые им операции всем своим имуществом (следует подчеркнуть, что лично нотариус, а не его нотариальная контора), а люди, выдающие паспорта, до сих пор являются работниками силовой структуры, со всей вытекающей ответственностью их перед законом.

К сожалению, следует отметить, что качество работы созданной системы УЦ недостаточно высокое. Так, например, Минкомсвязь, проверив в прошлом году всего 9 УЦ, сразу лишило двух из них аккредитации и еще у одного она приостановлена (30% от общего числа, что является крайне тревожным показателем). Добавим, что готовность сервисов проверки выданных таким большим количеством УЦ сертификатов составляет на практике около 80–85%, то есть в ряде случаев сертификат быстро проверить невозможно, а большое количество квалифицированных и неквалифицированных сертификатов просто не принимаются некоторыми сервисами. Поэтому набирает силу движение по созданию при некоторых системах электронного взаимодействия доверенных УЦ, создающих свои, выделенные в рамках общего пространства, «сегменты доверия».

Совершенно очевидно, что управление работой такого большого количества УЦ и обеспечение надлежащего качества их деятельности — объективно сложная задача, требующая приложения огромных усилий со стороны регулятора

Вывод напрашивается один — работа УЦ в целом организована неудовлетворительно и по некоторым параметрам является рискованной. Также совершенно очевидно, что управление работой такого большого количества УЦ и обеспечение надлежащего качества их деятельности — объективно сложная задача, требующая приложения огромных усилий со стороны регулятора. Для сравнения, Банк России решал в некотором сходную по размеру задачу по повышению уровня информационной безопасности в кредитных организациях в течение почти 10 лет и в конце концов ему пришлось резко усилить нормативное регулирование этой деятельности. Понятно, что в этих условиях говорить о создании единого пространства доверия на основе квалифицированных сертификатов, выданных аккредитованными удостоверяющими центрами, а значит

и универсальных сервисов электронного взаимодействия по крайней мере, преждевременно.

ВОКРУГ КЛЮЧА ПОДПИСИ

2. В полный рост возникает задача более гибкого и эффективного управления использованием ключа подписи, что потребовало отдельной проработки вопроса со стороны Минкомсвязи, вылившейся в идею выдачи хранящегося централизованно дополнительного квалифицированного «Уполномоченного» сертификата. Подготовлен соответствующий проект федерального закона.

Добавим, что не за горами возникновение задачи управления статусом документа, например, правами на объект, который зафиксирован в самом документе. В случае решения задачи управления собственностью это означает разделение объекта собственности и собственника, владеющего этим объектом (собственник может меняться, а зафиксированный в реестре БТИ или в ФНС объект собственности продолжает существовать в неизменном виде). Подобная задача может быть, к примеру, решена применением так называемого «атрибутивного» сертификата документа. Но все эти дополнения означают серьезное усложнение технологии электронного документооборота и электронного взаимодействия, не говоря уже об организации архивного хранения документов в электронном виде. Этот вопрос требует глубокой и тщательной проработки.

Все сказанное усложняется отсутствием удовлетворительных решений по мгновенному, в реальном масштабе



времени, отзыву и уничтожению ключа подписи в случае утраты владельцем ключа подписи либо полномочий на его использование, либо утраты им дееспособности. Нельзя сказать, что эта задача новая. Она известна и решается в бумажном документообороте, но почему-то в электронном взаимодействии пока удовлетворительного решения нет.

ТЕНЬ ПРЕЗИДЕНТА

3. Все больше вызывает вопросов практическое использование самой электронной подписи. В извечной борьбе между безопасностью, простотой и трудоемкостью использования этого инструмента доверия к электронному документу, похоже, начинает побеждать простота и дешевизна. Уже прошло десять лет с тех пор, как Президент Российской Федерации поставил задачу «окончательно разобраться с использованием электронной подписи», уже даны поручения решить вопрос о бесплатной выдаче всему населению страны средств электронной подписи (имеется в виду усиленная квалифицированная подпись), а на практике мы наблюдаем массовый интерес граждан к использованию простой или неквалифицированной электронной подписи и прежде всего потому, что это удобно, гораздо проще и ничего не стоит. При этом, в некоторых службах соотношение в использовании усиленной неквалифицированной и квалифицированной подписи достигает уже 95% к 5%, не говоря уже о том, что доступ к личным кабинетам (в ЕПГУ, налогоплательщика в ФНС, сдачи отчетности в Банке России и т.д.), в том числе к сервисам облачной подписи, осуществляется с помощью инструмента, поразительно похожего на простую электронную подпись. Можно предположить, что подобный механизм через некоторое время станет весьма и весьма распространенным. Видимо, необходимо обратить внимание на разработку механизмов обеспечения доверия к простой электронной подписи для повышения уровня ее безопасности при массовом практическом использовании.



К ИНфраСТРУКТУРЕ ДОВЕРИЯ

4. Наконец, о доверии в цифровом мире. Становятся заметными различия в использовании этого понятия. Применительно к правовым, техническим и организационным сторонам общего процесса различаются:

- ◆ доверие к электронному документу в гражданском процессе, включая его архивное хранение;
- ◆ доверие к технологическому средству обеспечения доверия к электронному документу — электронной подписи;
- ◆ доверие к статусу квалифицированной подписи, обеспечиваемое УЦ;
- ◆ доверие к сертификату электронной подписи;
- ◆ доверие к процедурам идентификации, аутентификации и авторизации;
- ◆ доверие к стандартам электронной подписи, хэш-функции, стандартам и сертификатам ключей шифрования, протоколам взаимодействия т.д.

То есть, следует очевидно говорить о наличии целой инфраструктуры доверия как отдельной сущности, требующей внимания специалистов как технического, так и гуманитарного, юридического профиля.

О ЧЕМ ГОВОРИЛИ ЗАРУБЕЖНЫЕ КОЛЛЕГИ?

При этом, наши зарубежные коллеги отмечают крайнюю важность наличия универсального идентификатора (ID) как базового инструмента для реализации процедур идентификации и аутентификации личности, использования

электронной подписи во всех ее вариантах, включая мобильную и облачную подписи, работы с базами данных и с архивами документов. Так, в Европейском Союзе в 2018 году запланировано введение единого аутентификатора, создание единого реестра таких аутентификаторов (eIDAS) и сопоставления с ними наборов «услуг доверия», предоставляемых физическим лицам — гражданам ЕС: сертификатов, штампов времени и т.д. Не отстает от них и Республика Азербайджан, запустившая в этом году универсальный мобильный сервис идентификации и электронной подписи. Представляется, что этот опыт целесообразно внимательнейшим образом изучить, а может быть и рассмотреть возможность принятия, естественно с учетом наших особенностей.

* * *

И что крайне отраднo, вновь начинает подниматься затихший было вопрос о необходимости подготовки Федерального закона «Об электронном документообороте» или «Об инфраструктуре доверия к электронным документам», а вместе с ним — вопрос об официальной электронной почте или электронном взаимодействии, официальных электронных адресах, едином ID, как это уже упоминалось, терминологии и определениях. Хочется верить, что следующий РКИ-Форум даст ответы на некоторые из поставленных вопросов.



КАКИМ МОЖЕТ БЫТЬ ЗАКОН ОБ ЭЛЕКТРОННОМ ДОКУМЕНТЕ

Он должен учитывать юридическую сущность документа вообще, и электронного документа в частности

10 марта 2016 года в Москве в ходе семинара, посвященного проблемам электронного документооборота, были поставлены актуальные общесистемные и нормативные вопросы применения электронных документов.

Представляется правильным сделанный экспертами акцент на том, что развитие федеральной законодательной базы в сфере ЭДО пока явно недостаточное¹.

В настоящее время разнообразные юридические действия совершаются (или должны совершаться) в электронном виде путем использования электронных документов. Применение электронных документов в юридических целях требует специального правового механизма. Такой механизм должен однозначно определить условия, при которых электронный документооборот между субъектами с различным правовым статусом: частными физическими и юридическими лицами, органами государственной власти, муниципальными органами, имеет юридическую силу и влечет правовые последствия; установить институты и процедуры, задействованные при осуществлении электронного документооборота, а также урегулировать общие вопросы правового режима электронных документов, в том числе в закрытых системах.

В этих целях требуется разработка и принятие Федерального закона «Об электронном документе (документоо-

бороте)», который должен учитывать юридическую сущность документа вообще, и электронного документа в частности.

Традиционно документ определяется как деловая бумага, подтверждающая факт или право на что-либо, способная служить письменными, в том числе судебными доказательствами юридических отношений и событий, и рассматривается правоведами как способ оформления правовых отношений.

В информационном обществе юридическая трактовка документа изменилась и сосредоточилась не на фиксации в нем правового отношения, а на выявлении взаимосвязи документа (прежде всего электронного) и информации. Электронный документ стал трактоваться как информация, обладающая установленными реквизитами и представленная в электронной форме.

При таком подходе утратился юридический смысл и юридическая функция электронного документа, из него было исключено правовое отношение и стало непонятно, на каком основании он должен вызывать те же правовые последствия, что и документ бумажный.

В качестве такого основания должен служить разработанный UNCITRAL правовой принцип функционального эквивалента, который используется в области электронной торговли, электронной подписи, электронных передаваемых записей.

В соответствии с данным принципом в законодательстве устанавливаются требования, которым должен удовлетворять электронный документооборот для того, чтобы он отвечал тем же юри-

дическим целям и функциям, которые выполняются в традиционной бумажной системе.

Законом «Об электронном документе (документообороте)» должен быть создан правовой механизм, обеспечивающий функциональный эквивалент — гарантирующий, что электронный документооборот будет фиксировать правоотношение, т.е. даст тот же юридический результат, что и документ бумажный.

Указанный правовой механизм следует конструировать путем законодательного оформления «инфраструктуры доверия электронным документам», в рамках которой уполномоченные лица — провайдеры совершают юридические действия по оказанию доверенных услуг: выполняют подтверждающие, устанавливающие личность, регистрационные, доказательственные функции, влияющие на действительность, статус и форму электронных документов.

Доверенными услугами являются: создание, проверка, подтверждение электронных подписей и сертификатов, электронных печатей, электронных штампов времени, электронных документов, а также электронная доставка документов и сообщений, удостоверение подлинности вебсайтов и др.

Юридические конструкции доверенных услуг (сервисов), пространства доверия, субъектов и сервисов доверенной третьей стороны зафиксированы в европейских и евразийских правовых документах: в Постановлении (ЕС) № 910/2014 Европейского парламента и Совета «Об электронной иденти-

¹ «Как скоро электронный документ заменит бумажный» // BIS Journal – Информационная безопасность банков 02/2016, с.14–19



кации и доверенных услугах для электронных транзакций на внутреннем рынке и отмене Директивы 1999/93/ЕС»; в Договоре о Евразийском экономическом союзе (Протоколе об информационно-коммуникационных технологиях и информационном взаимодействии).

В законе «Об электронном документе (документообороте)» необходимо закрепить положение о том, что юридическое признание электронных документов по сути является признанием юридической роли доверенных услуг и субъектов, которые такие услуги оказывают.

Закон должен состоять из двух частей — общей (институциональной) и особенной (функциональной).

Общая часть посвящена основным положениям о доверенных услугах, лицах, которые их оказывают (провайдерах) и электронных документах (включая электронные подписи, электронные печати, электронные штампы времени, сертификаты и т.д.).

Общая часть включает также базовые принципы: технологической нейтральности законодательства; функциональной эквивалентности; защиты персональных данных и т.п.

В законе следует предусмотреть:

- ♦ открытый перечень доверенных услуг и общие требования к ним (к безопасности, надежности и др.);
- ♦ общие условия признания доверенных услуг, в том числе в качестве судебных доказательств;
- ♦ юридические различия между квалифицированными и неквалифицированными доверенными услугами;

- ♦ особенности правового статуса надежных поставщиков доверенных услуг и требования к ним.

В общей части должны быть сформулированы:

- ♦ условия признания юридической силы электронных документов и иных электронных записей, электронных подписей, электронных печатей, электронных штампов времени;
- ♦ положения о юридической силе квалифицированной электронной подписи, квалифицированного сертификата;
- ♦ правовой режим электронной официальной доставки и хранения электронных документов.

Особенная, функциональная часть предусматривает юридические условия функционирования доверенных сервисов в зависимости от сферы применения электронного документа.

1. Административная сфера и публичные услуги. Правовой механизм характеризуется государственным регулированием и контролем.

Включает:

- ♦ условия признания электронной идентификации и доверенных услуг институтами, органами, ведомствами и учреждениями, в том числе в сфере публичных услуг, оказываемых частным лицам;
- ♦ особенности функциональной эквивалентности электронной и письменной формы документов и иных записей в административной сфере и сфере публичных услуг;
- ♦ использование электронных документов, подписанных квалифицированной электронной подписью; сертифици-

рованных средств квалифицированной электронной подписи; квалифицированных поставщиков доверенных услуг;

- ♦ ответственность квалифицированных поставщиков;
- ♦ систематический государственный контроль за деятельностью квалифицированных поставщиков.

2. Сфера электронной торговли. Правовой механизм характеризуется договорными отношениями и элементами государственного контроля.

Включает:

- ♦ свободу договора и не дискриминацию при использовании электронных документов, квалифицированных и неквалифицированных электронных подписей, сертификатов, квалифицированных или неквалифицированных доверенных услуг;
- ♦ особенности функциональной эквивалентности электронной и письменной формы документов и иных записей;
- ♦ особенности реализации принципа технологической нейтральности правовых норм и требований;
- ♦ возможность ограничения ответственности поставщиков доверенных услуг;
- ♦ страхование финансовых рисков поставщиков доверенных услуг;
- ♦ ограниченный государственный контроль.

3. Правовые отношения в закрытых системах. Основаны на саморегулировании и оказывают воздействие только на участников таких систем, но не третьих лиц:

- ♦ регулирование осуществляется для управления внутренними процессами самими участниками, которые устанавливают правила системы, включающие санкции за нарушение правил и механизмы разрешения конфликтов;
- ♦ участники системы действуют, исходя из автономии воли, в своем интересе и на свой страх и риск;
- ♦ саморегулирование осуществляется на легитимной основе, применяются законодательно не запрещенные инструменты и конструкции.

INFOSECURITY RUSSIA 2016

МЕНЬШЕ, ДА ЛУЧШЕ

Выставка показала, что сфера информационной безопасности в России имеет твердое здоровое ядро и тенденцию к росту

В Москве в выставочном центре «Крокус Экспо» завершилась XIII Международная выставка InfoSecurity Russia. Она безусловно подтвердила свой статус авторитетного и масштабного события в жизни отрасли.

Любопытно, что некоторое сокращение в связи с кризисом числа участников и выставочных площадей парадоксальным образом только усилило выставку, в этом году она, словно сбросив жирок, стала более активной, организованной, наступательной. Да, участников было меньше, но посетителей, контактов, контрактов — заметно больше!

Посетители шли потоком, и не зря. Феерическое шоу кружило и поражало. Яркие полуобнаженные девы завлекали на стенды с металлическими ящиками криптомодулей и сетевых экранов, Медиа Группа «Авангард» осыпала лучших ИБ-шников золотыми желудями, легендарные представители элиты ИБ рассказывали в микрофон профессиональные и политические анекдоты, а в гигантской стеклянной будке в центре зала неистовый тележурналист В. Былевский доводил собеседников своими вопросами буквально до экстаза...

Вся эта праздничная мишура, создающая приподнятое настроение, только помогала ощутить рабочее напряжение

форума. На стендах безостановочно проводились презентации, обсуждались проекты, совершались сделки, а на многочисленных открытых и закрытых площадках без остановки, словно гудит ток по электрическим проводам, шел титанический мозговой штурм: 8 индустриальных конференций, 11 тематических секций, 3 семинара, 2 круглых стола, 28 выступлений в зале коммерческих презентаций, 155 докладов — такая вот программа семинаров и тайм-слотов в режиме нон-стоп.

Обход выставки по стендам и павильонам с микроопросом участников — такое легкое социологическое сканирование — только подтверждает общее впечатление.



Звёздные гости пресс-рума дают интервью телекомпании BIS TV: поэт Владимир Вишневский, балетмейстер Сергей Филин, музыкант и композитор Владимир Пресняков-старший





Мария Лурье,
ООО «С-Терра СиЭсПи»:

— Мы участвуем в этой выставке с самого начала. Кризис не обошел ее стороной, и на этот раз тут меньше экспонентов, но она не стала от этого менее интересной, скорее наоборот: более шумная, живая. Серьезная конференц-часть, полезные доклады. Удачное нововведение — дни выставки разделили по темам: первый день — промышленная безопасность, второй — финансовая, третий — безопасность виртуальной среды. Это удобно. Можно спланировать аудиторию, которую ожидаешь в гости на стенд, подготовиться, подобрать материалы.

— Что для вас является мерилом эффективности выставки?

— Хочется ответить, «количество «лидов», как это сейчас модно, но нет. Скорее количество полезных контактов, причём не только с новыми партнёрами, но и с давними. Выставка — это удобное место для встреч и в то же время особое информационное поле. Плюс на других посмотреть — тоже очень полезно.

— Что на этот раз показалось наиболее интересным?

— В этом году много докладов на каждом стенде. Я не про конференц-часть, а про мини-семинары прямо на стендах.

— Какая тема была у вас?

— Мы провели пять семинаров. Решения в телеком-секторе, финансовом секторе. Рассказывали про универсальные криптомаршрутизаторы — это целая линейка наших новых разработок, про защиту связи между цодами...

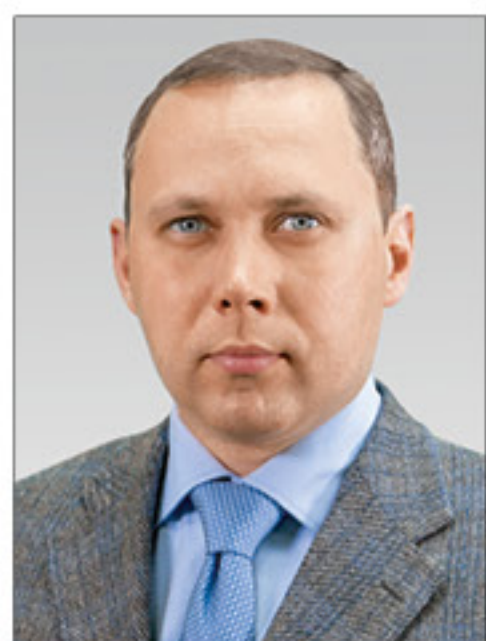
Дмитрий Лебедев,
компания Altell

— На этой выставке я впервые. Тут комфортно. Я бы назвал ее Выставкой импортозамещения, так как тут много отечественных разработчиков со своими продуктами. Мы из Питера и тоже представляем свои разработки: межсетевой экран и модуль доверенной загрузки. Время провели с пользой: договорились о сотрудничестве с коллегами и, надеюсь, нашли заказчика. К нам подошли представители одного министерства и сказали, что хотели бы с нами работать.

Андрей Баранов,
руководитель представительства
компания Gigamon в России

— Принимаю участие в выставке с 2013 года. Тогда она была масштабнее, но в этом году интерес к ней заметно вырос, по крайней мере, по сравнению с прошлым годом. Сама выставка тоже изменилась: на ней появились вендоры. В 2014–2015-м годах их было значительно меньше. А сейчас посмотрите, вот стенды Gigamon, Vmware, Фортинет, Нетскаут... — все они представляют решения в области информационной безопасности. И это говорит о том, что и западные, и восточные вендоры ощущают, что российский рынок пошел в рост.

Более того, системные интеграторы, которые также работают в области информационной безопасности — «АМТ-груп», «Информзащита» и другие, можно сказать, костяк информационной безопасности России, — тоже серьезно представлены на этой выставке. Что также укрепляет веру в рост российского рынка.



Артем ЗУБКОВ
генеральный директор
Медиа Группы
«Авангард»

ИГРА НА ОПЕРЕЖЕНИЕ

Медиа Группа «Авангард» открыла интернет-портал bisjob.ib-bank.ru, посвященный вопросам образования и карьеры в сфере информационной безопасности

Новый портал так и называется — «Образование и карьера». Он стал очередным этапом в развитии большого проекта Медиа Группы «Авангард» по информационному обеспечению отрасли (журнал «BIS Journal — Информационная безопасность банков», отраслевой портал ib-bank.ru, интернет-телекомпания BIS TV, издание книг и трудов по отраслевой тематике, конференции и форумы).

Формирование кадрового потенциала любой наукоемкой отрасли относится к числу стратегических задач и обладает инерционностью в годы, а порой и десятилетия. С учётом динамичного развития технологий и обновления нормативно-правовой базы специалистам нужно своевременное повышение квалификации, а в отдельных случаях и переподготовка. Не является исключением и сфера ИБ, нуждающаяся в системе непрерывного образования. В идеале она должна начинаться со школьной скамьи, продолжаться в вузах и далее в профильных учебных центрах. Следует отметить, что в нашей стране элементы этой системы во многом уже готовы.

На уровне среднего общего образования проводятся межрегиональные олимпиады школьников по криптографии, по компьютерной безопасности, функционируют специализированные физико-математические школы и классы, проводится профессиональная ориентация старшеклассников на получение высшего образования по профилю ИБ.

На уровне профессионального образования обучение ведется по линейке из 10 федеральных государственных образовательных стандартов в вузах и трех — в техникумах. Координацию работы и обеспечение единства образовательного пространства осуществляют профильные федеральные учебно-методические объединения в сферах среднего профессионального и высшего образования. Во время обучения студенты начинают готовиться к грядущей трудовой деятельности. Они устанавливают связи с государственными и коммерческими организациями, проходят производственную практику, работают по совместительству, пишут по итогам дипломные работы.

После получения диплома, накопив опыт работы, специалисты по информационной безопасности могут повысить свою квалификацию в профильных учебных центрах, созданных на базе вузов или независимых. Это позволяет не только приобрести новые компетенции, но и создает предпосылки для карьерного роста. Кроме того, это необходимо работодателям для осуществления лицензируемых видов деятельности, а также в связи с вводимыми в Российской Федерации профессиональными стандартами для специалистов в сфере информационной безопасности и защиты информации. Данные стандарты также вскоре станут ориентирами для подготовки специалистов в вузах и поствузовского обучения.

Объединение этих трех составных частей в целостную систему поможет обеспечить сбалансированность рынка труда, преодолеть дефицит специалистов необходимой квалификации. Новый портал «Образование и карьера» Медиа Группы «Авангард» создан для содействия в достижении этой цели.

Этот информационный ресурс подготовлен и будет работать усилиями многих партнёров. Среди них:

- ♦ МОО «Ассоциация защиты информации»;
- ♦ Оргкомитеты олимпиад школьников по криптографии и по компьютерной безопасности;
- ♦ Профильные федеральные учебно-методические объединения в областях

Миссия сайта «Образование и карьера» — информационно-аналитическая поддержка непрерывного образования как важнейшего фактора кадрового обеспечения сферы информационной безопасности России



Кадровая стратегия — это всегда игра на опережение, она жизненно необходима для развития отечественной отрасли информационной безопасности

среднего профессионального и высшего образования;

♦ ряд отраслевых образовательных организаций.

Миссия сайта «Образование и карьера» — информационно-аналитическая поддержка непрерывного образования как важнейшего фактора кадрового обеспечения сферы информационной безопасности России. Представляемые на нем различные публикации и материалы предназначены как для тех, кто находится в начале профессионального пути, так и для тех, кто по праву может считаться экспертом.

Структура и функции портала соответствуют классификации ступеней образования.

Первая из них — «Школьники» — посвящена выбору профессии и подготовке к поступлению в вуз. Материалы раздела рассказывают о возможностях системы среднего общего образования в различных регионах: профилированных классах, специализированных школах, интеллектуальных состязаниях в области ИБ. Интересующиеся школьники могут решать увлекательные задачи, знакомиться с популярной литературой об истории криптографии,

узнавать о предстоящих тематических культурно-массовых мероприятиях. И, главное, ознакомиться с имеющимися профильными вузами и выбрать, куда поступать. Планируется вести рейтинг таких вузов.

Вторая ступень — «Студенты» — посвящена содействию в трудоустройстве выпускников. В этом разделе содержатся материалы о вузах, готовящих специалистов по информационной безопасности и защите информации. Будет расширяться информация об учебных заведениях, научно-педагогических школах, лучших студентах и преподавателях. Студенты смогут принять участие в интеллектуальных соревнованиях, узнать об особенностях научной работы, производственной практике, подработках и трудоустройстве.

И третья, «высшая» ступень — «Специалисты» — содержит материалы о карьере и поствузовском профессиональном образовании — повышении квалификации и профессиональной переподготовке. Раздел будет обновляться актуальными требованиями к специалистам по информационной безопасности и защите информации. Кроме того, периодически будет появляться аналитика о рынке труда, информация о вакансиях и предложения резюме. Все желающие смогут найти информацию о профильных образовательных организациях, обучающих и деловых отраслевых мероприятиях.

В заключение ещё раз подчеркнем: отраслевая кадровая стратегия — это всегда игра на опережение, она жизненно необходима для развития отечественной отрасли информационной безопасности. А система этих последовательных ступеней непрерывного образования «школа — вуз — повышение квалификации» помогает становлению настоящих профессионалов, способных не только идти в ногу со временем, но и формировать задел на будущее.



ЛОГИКА ПОБЕДЫ

Цель олимпиад — привлечение одаренных школьников в сферу ИБ

На X Съезде Российского союза ректоров отмечалось, что одной из важнейших задач российской высшей школы является обеспечение эффективного функционирования общенациональной системы работы с молодыми талантами. Необходимо развитие механизмов поиска, выявления, поддержки и сопровождения таланта с помощью среды из обучающих и мотивирующих, побуждающих к будущей профессиональной деятельности программ и проектов, а также совершенствование государственной информационной политики по популяризации достижений российской науки, обеспечению свободного доступа к информационным ресурсам по работе с талантливой молодёжью и подготовке к интеллектуальным мероприятиям.

Такая работа должна быть организована в интересах каждой наукоемкой и высокотехнологичной сферы деятельности, в том числе и в отрасли информационной безопасности.

В России существует система интеллектуальных соревнований для школьников и студентов в данной сфере. Ее формирование стартовало более четверти века назад, с начала проведения Межрегиональной олимпиады школьников по математике и криптографии. В настоящее время аналогичные олимпиады по компьютерной безопасности проводятся для школьников и для студентов, обучающихся по профильным специальностям. Также в последние несколько лет набирают популярность соревнования студентов в формате CTF.

Рассмотрим подробнее указанные олимпиады. С самого начала логика их проведения определялась четко по-

ставленной целью — привлечь внимание наиболее талантливых и математически одаренных школьников к информационной безопасности как будущей сфере профессиональной деятельности. Это обстоятельство наложило свой отпечаток на состав заданий олимпиад. Они, с одной стороны, должны были базироваться на школьной программе, а с другой, помогать выявлять у школьников заинтересованность и склонность к решению стоящих перед отраслью ИБ проблем. Создание фонда таких задач и его ежегодное обновление можно считать самостоятельным научно-педагогическим направлением, достойным глубокого изучения, анализа и развития.

Такой подход в совокупности с проведением Олимпиад для учащихся разных классов, от 8 до 11, дополнил целевую функцию проведения мероприятий ознакомлением их участников с криптографией как наукой и повышением общей математической осведомленности. Кроме того, успешное участие школьника в олимпиадах, начиная с 8–9 классов, позволяет ему ежегодно обогащаться положительным опытом решения задач нарастающей сложности и приводит к осознанной заинтересованности тематикой защиты информации.

Формирование специалиста в сфере ИБ требует не только интенсивного усвоения школьной программы, но и выработки целого ряда квалификационных качеств, хорошо развитые которые поможет участие в олимпиадах. Отметим некоторые из этих качеств.

1. Умение формализовать задачу, проанализировать ее условия, построить для ее решения математическую модель.

2. Способность разработать поэтапный план решения, четко выделяя взаимосвязанные подзадачи, что в конечном итоге сблизит процесс решения с построением формального алгоритма и его реализацией.

3. Готовность привлечь для решения знания из различных разделов математики, информатики и физики, чего не хватает в школьном обучении, выстроенном преимущественно по тематическому принципу и страдающему выработкой шаблонов мышления.

4. Высокая творческая активность, при которой школьник не ограничивается подбором стандартных приемов, но способен отыскать совершенно новые пути решения.

5. Самостоятельность, основанная на необходимости рассчитывать исключительно на собственные силы и знания.

Как показывает практика, психология школьников такова, что даже однократный успех в развитии хотя бы одного из этих качеств в рамках Олимпиады получает устойчивое закрепление. Если функции воспитания интереса к отрасли информационной безопасности понятны, то над отражением специфических, присущих исключительно данному виду деятельности черт организаторы олимпиад творчески работают в каждом годовом цикле их проведения. Достичь желаемого результата удастся путем составления и тонкой настройки задач.

Постановки многих задач олимпиад — криптографические. Часть имеет криптографическую окраску, но их суть — математическая или алгоритмическая. Отдельные задачи — просто математические. Тематика предлагаемых задач весьма разнообразна.



Президентский зал РАН. Март 2016 года. Разбор задач XXV Межрегиональной олимпиады школьников по математике и криптографии и X Межрегиональной олимпиады по информатике и компьютерной безопасности

Задачи первых олимпиад по криптографии в основном были посвящены так называемым ручным шифрам, некоторые из которых применялись еще до нашей эры. Позднее появились задачи, в которых затрагивались и разделы современной криптографии, такие как криптосистемы с открытым ключом, стеганография, квантовая криптография и криптографические протоколы. Также возник цикл задач, относящихся скорее к области защиты информации, чем собственно к криптографии.

При составлении вариантов заданий олимпиад для различных возрастных категорий особое внимание уделяется оценке сложности задач и времени,

отводимому на их решение. Благодаря этому практически каждый год находят участники, решившие все задачи. При подведении итогов организаторы каждый год с удовлетворением отмечают наличие у отдельных участников оригинальных решений, более красивых, чем исходно предполагавшиеся составителями.

Стоит отметить, что подготовка заданий усложняется тем, что ежегодно разрабатывается три цикла сценариев: для 8–9, 10 и 11 классов — каждый со своей спецификой, но с сохранением связи между собой. К этой сложной работе привлекаются коллективы преподавателей, возглавляют ее опытные

и авторитетные специалисты. По итогам олимпиад ежегодно издаются сборники задач и решений.

Высокий уровень организационного и методического обеспечения олимпиад породил еще один феномен — большое внимание представителей отрасли к заключительному мероприятию олимпиадного цикла — подведению итогов и награждению победителей. Площадками для проведения таких мероприятий в разные годы выступали Президентский зал здания Президиума и Математический институт РАН, Художественная галерея А. М. Шилова и другие. Одна из причин такого внимания — осознаваемая всеми специалистами в области информационной безопасности потребность в ее популяризации.

Проводимые олимпиады дают системную основу для позиционирования отрасли информационной безопасности в современном обществе и привлечения школьников к развитию в направлении этой сложной, но исключительно интересной области науки и техники.

BIS-СПРАВКА

Межрегиональная олимпиада школьников по математике и криптографии. Проводится ежегодно с 1991 года Академией криптографии РФ совместно с Институтом криптографии, связи и информатики Академии ФСБ России, при участии Федерального учебно-методического объединения по направлению подготовки «информационная безопасность» и входящих в его состав вузов. Заключительный — очный этап Олимпиады проводится более чем в 40 субъектах РФ. С 2008–09 учебного года Олимпиада ежегодно включается в Перечень Минобрнауки, что позволяет вузам предоставлять ее победителям и призерам льготы при поступлении.

Председателем оргкомитета Олимпиады долгие годы является В. Н. Сачков — вице-президент Академии криптографии РФ. Методическую комиссию всегда возглавляли ведущие математики России: с 2008 по 2013 годы — академик РАН, академик Академии криптографии РФ Ю. В. Прохоров, с 2014 года — вице-президент РАН, директор Математического института им. В. А. Стеклова РАН, академик РАН, академик Академии криптографии РФ В. В. Козлов.

В настоящее время Олимпиада проходит в три этапа: ознакомительный, отборочный и заключительный. Кроме того, в течение всего года школьникам доступны on-line курсы подго-

товки к Олимпиаде. Сайт Олимпиады: www.cryptolymp.ru

Межрегиональная олимпиада по информатике и компьютерной безопасности. Проводится с 2006 года Институтом криптографии, связи и информатики Академии ФСБ России, при участии Федерального учебно-методического объединения по направлению подготовки информационная безопасность и входящих в его состав вузов. Председатель методической комиссии — академик РАН В. К. Левин. Входит в Перечень олимпиад Минобрнауки России с 2015 года. Очный этап проводится более чем в 20 городах России.



ГОТОВИМ КИБЕРДРУЖИНУ!



Начну с очевидного: в обозримом будущем профессия специалиста по информационной безопасности останется одной из самых рейтинговых. Она будет востребована и государственными, и общественными структурами и, разумеется, бизнесом, в особенности — банками и другими финансовыми институтами. Сегодня же ситуация на рынке труда характеризуется огромной нехваткой профессионалов. Доля вакантных мест на должность специалиста по кибербезопасности на мировом рынке составляет 25–30% от всех вакансий. Думаю, что в России этот показатель ещё выше.

Зачем Сбербанк создает свою программу подготовки кадров по информационной безопасности

Не менее очевидно и то, что уровень подготовки специалистов этой сферы российскими вузами не соответствует запросам работодателей. Знания устаревают стремительно, многие теоретические предметы никогда не потребуются на практике. Беды российского образования известны, их устранение, создание гибкой, чутко улавливающей требования времени системы подготовки кадров — задачи профессионалов из Министерства образования. Пока же такой системы нет, и нам остаётся либо искать готовых специалистов на рынке и затем адаптировать их к условиям работы, либо, исходя из своих потребностей, самим выстраивать схемы взаимодействия с высшей школой по подготовке нужных людей.

Исходя из этой идеи, Сбербанк подписал стратегическое соглашение с ведущими российскими вузами о сотрудничестве в сфере информационной безопасности. В список вошли МГУ им. М. В. Ломоносова, МИФИ, Финансовый университет при Правительстве Российской Федерации, МГТУ им. Н. Э. Баумана, Московский университет МВД им. В. Я. Кикотя, МИЭМ (ВШЭ) и МФТИ. Сбербанк готов оказать помощь в коррекции учебных планов, формировании лабораторной базы и представлении современного банковского оборудования; готов участвовать в формировании перечня актуальных тем курсовых и дипломных работ, а также проведении занятий для студентов, в том числе на базе Сбербанка.

Пунктов у соглашения много, есть положения и об именных стипендиях лучшим студентам и предоставлении возможности прохождения практики и последующего устройства лучших студентов на работу. Кроме этого, предусмотрена возможность выделения средств вузам на проведение исследовательской работы.

Чего мы ждём взамен: профессионалов в области управления различными процессами кибербезопасности, готовых сразу включиться в рабочий процесс.



Мастер-класс, прошедший в Сбербанке 10 сентября 2016 года

Интересным мероприятием в рамках соглашения станет цикл мастер-классов под общим названием «Практические вопросы информационной безопасности банковской системы». Спикеры — ведущие специалисты российской отрасли кибербезопасности. Они представляют такие компании, как Microsoft, АО «Национальная система платёжных карт», PricewaterhouseCoopers, НП «Национальный совет финансового рынка», конечно, Сбербанк, вуз-партнёры.

Темы обучающих программ охватывают широкий спектр практических вопросов. Организация безопасности сетевого взаимодействия и безопасность «облачных» технологий; нюансы использования DLP и организация процесса расследования инцидентов ИБ; применение криптографических технологий в банковских АС и организация защиты от DDoS-атак; юридические аспекты и экономика информационной безопасности. Это далеко не полный перечень. Мастер-классы будут проводиться практически каждую субботу с 10 до 14 часов, начиная с 10 сентября и заканчивая 27 мая. Адрес площадки — центральный офис Сбербанка в Москве на ул. Вавилова, 19, конференц-зал.

Кого мы ждём на этих курсах? Молодых людей, которые интересуются современными подходами в сфере кибербезопасности. Тех, кто хочет научиться строить математические модели для противодействия мошенничеству. Тех, технических специалистов, которые узнают не только как, но и почему работает та или иная «железка». Специалистов, которые смогут грамотно готовить документацию и описывать процессы, составлять метрики. Экспертов, которые будут анализировать код программного продукта на предмет его безопасности. Регистрация проходит на кафедрах вузов. Её можно также пройти самостоятельно на кадровом портале Сбербанка <https://sberbank-talents.ru/info/cybersecurity/>.

В общем, Сбербанк начал создавать программу подготовки кадров по информационной безопасности. У этого процесса есть и ещё одна сторона. Каждый молодой человек, разбирающийся в вопросах кибербезопасности, станет своеобразным «агентом влияния», проводником культуры информационной безопасности в обществе. Сейчас этой культуры, увы, не хватает.

Доля вакантных мест на должность специалиста по кибербезопасности на мировом рынке составляет 25–30 % от всех вакансий. Думаю, что в России этот показатель ещё выше



Марина БРОДСКАЯ
обозреватель BIS Journal

МНОГО ЛИФТОВ НА ОЛИМП

*Обзор профильных соревнований
для студентов и молодых специалистов*

Как правило, студенческие олимпиады проводятся «с целью выявления и развития творческих способностей, интереса к научной деятельности, создания условий для интеллектуального развития...» и т.д. и т.п. Но не все так скучно. За казенными формулировками порой скрываются не просто занимательные, а поистине судьбоносные события. Например, победители и призеры автоматически проходят в магистратуру, получают работу в компании с мировым именем или поддержку своему драгоценному стартапу, не говоря уж о такой мелочи, как гранты, стажировки, денежные призы...

СТУДЕНЧЕСКИЕ ОЛИМПИАДЫ

В 2017 г. пройдет уже V Всероссийская студенческая олимпиада по информационной безопасности. Она проводится Минобрнауки, ФСТЭК, УМО высших учебных заведений России по образованию в области информационной безопасности, НИЯУ МИФИ. Сегодня это одно из базовых мероприятий по выявлению и поддержке талантливых студентов, и соответственно один из самых мощных профессиональных и социальных лифтов в сфере ИБ. В 2016 г. в ней участвовали 133 студента из 38 российских университетов, плюс студенты из Беларуси, Украины, Кыргызстана и Казахстана. Лидировали команды МИФИ, МИЭТ и Южного федерального университета.

А 13–21 ноября в Новосибирске пройдет III Международная студенческая

олимпиада NSUCRYPTO-2016. Ее организаторы — университеты Новосибирска, Томска, Белорусский госуниверситет и Университет Левена (Бельгия) — хотят привлечь внимание студентов и школьников к современной криптографии. В первом туре все желающие, зарегистрировавшиеся на сайте организаторов, получают задания на английском языке и 4,5 часа будут решать несколько задач, не требующих специальных знаний. Во втором туре предлагается ряд сложных и нерешенных задач по криптографии и криптоанализу. Решение некоторых из них можно рассматривать как серьезное личное достижение. Победителям же олимпиады карьера, как минимум, академическая, обеспечена.

СКОЛКОВО: КОНКУРС ПРОЕКТОВ

15 ноября завершается прием заявок на участие в Skolkovo Cybersecurity Challenge — международном конкурсе инновационных проектов, направленных на защиту мира от киберугроз. Приглашаются как отдельные исследователи и независимые команды, так и малые, и средние технологические компании. Участие в конкурсе позволит получить финансирование для реализации технологии, найти партнеров, клиентов, создать новую компанию. Призовой фонд конкурса — несколько миллионов рублей — может быть увеличен по решению жюри.

Также участникам гарантируются спецпризы от партнеров конкурса — компаний Cisco, Лаборатории Касперского, LETA Capital, сертификаты на обучение по магистерской программе по веб- и об-

лачной безопасности, встречи с командой Almaz Capital, включение проекта в дорожную карту Национальной технологической инициативы SafeNet и др.

СТФ: КИБЕР-БИАТЛОН В МОСКВЕ И ПЕЙНТБОЛ В ТОМСКЕ

В этом году Третьи Московские межвузовские соревнования М*СТФ по информационной безопасности пройдут в новом формате. Вместо традиционного Task-Based CTF будет Кибер-Биатлон. Он пройдет с 19 часов 9 декабря по 19 часов 11 декабря. В течение двух суток участникам предстоит выполнить ряд лабораторных работ и ответить на вопросы тестов по разным направлениям информационной безопасности. Игры пройдут в режиме онлайн, и принять участие в них сможет любой желающий.

Соревнования по информационной безопасности в формате CTF проводятся по всей России. В октябре, например, в Новосибирске проходят соревнования KrasCTF на базе Сибирского федерального университета при поддержке АРСИБ, а в С.-Петербурге — SpbCTF-2016 на базе Университета ИТМО при поддержке Центра специальных разработок Министерства обороны РФ.

Весной пройдут Открытые региональные соревнования NSK CTF на базе того же Сибирского федерального университета, во Владивостоке на острове Русский на базе ДВФУ традиционно пройдут соревнования DvCTF, в Екатеринбурге на базе Уральского федерального университета — RuCTF,



Победители и призеры автоматом проходят в магистратуру, получают работу в компании с мировым именем или поддержку своему драгоценному стартапу, не говоря уж о такой мелочи, как гранты, стажировки, денежные призы...

в Омске на базе ОГУ — ОмCTF. Летние соревнования традиционно проходят на Алтае — AltayCTF.

Соревнования VolgaCTF-2016, завершившиеся в сентябре, просто поразили своим масштабом. В отборочном этапе в режиме онлайн приняли участие 668 команд из 65 стран мира. К участию в очном финале в Самаре были приглашены 5 команд из ПФО, 5 команд из других регионов РФ, 4 команды и научная рота Минобороны России, команды из университетов Германии, США, Швейцарии и Казахстана.

Также в сентябре в Томске состоялись SibirCTF. Эти удивили неожиданной программой. Битва тут развернулась не только в виртуальной реальности, но и на открытой местности, где участникам пришлось побегать по нежилому району, вооружившись пейнтбольными ружьями.

POSITIVE HACK DAYS: ХАКЕРАМ НА ЗАМЕТКУ

Секция PHDays Young School проходит в рамках международного форума Positive Hack Days с 2012 г. Молодым специалистам предоставляется уникальная воз-

можность проводить самостоятельные исследования и общаться с ведущими экспертами в области информационной безопасности. Чтобы попасть в Young School, надо представить краткие тезисы по практическому направлению информационной безопасности, обосновать актуальность работы и описать результаты экспериментального исследования.

Авторы лучших работ получают возможность выступить перед хакерами и специалистами по безопасности на очередном международном форуме Positive Hack Days, который традиционно проходит в Москве весной. Помимо деловых встреч и докладов на тему ИБ, командам участников предлагают принять участие в соревнованиях CTF и на практике «взломать» промышленные объекты, финансовые организации и все, что только придет в голову организаторам.

МНОГО-МНОГО МЁДА...

Стоит отметить, что поддержку студентам и молодым ученым оказывают многие вузы и компании. Открытый конкурс на лучшую студенческую работу в области ИБ проводит ИКСИ Ака-

дамии ФСБ РФ. Недавно ГК «Инфотекс» объявила о программе поддержки и развития научного сообщества России в области информационной безопасности и криптографии «ИнфоТеКС Академия». Участие в ней даёт возможность получить поддержку оригинального исследовательского проекта и довести его до реализации.

1 октября стартовала X Юбилейная Международная олимпиада в сфере информационных технологий «IT-Планета 2016/17», в ней могут участвовать студенты, молодые специалисты и учреждения высшего и среднего профессионального образования любой страны мира. Регистрация участников начнется 1 ноября 2016 г., срок ее окончания зависит от номинации. Финал олимпиады пройдет в конце мая 2017 г. в Сочи. Вопросы ИБ включены в номинацию «Телеком», которую курируют Cisco, Huawei, D-Link.

...И ЛОЖЕЧКА ДЕГТЯ

Впрочем, не все организации, имеющие сайты и предлагающие принять участие в олимпиаде, являются тем, за кого себя выдают. Поэтому нужно помнить, что дистанционное участие в олимпиадах и конкурсах молодых специалистов — всегда бесплатное. При участии в очных этапах организаторы, как правило, берут часть расходов на себя, а участники оплачивают проезд до места мероприятия.

В процессе поиска информации мне попадались и сайты, которые предлагают за символический взнос ответить на 10 вопросов по любому школьному предмету (варианты ответов предлагаются) и в течение суток скачать уже готовый диплом с указанием фамилии и имени участника, синей печатью организатора и указанием номинации... Ценность такого диплома, конечно, меньше оплаченного взноса, но беда даже не в этом. Предлагаемые на сайте заархивированные материалы часто содержат вирус, поэтому сложно сказать, во сколько на самом деле обойдется участнику такой «олимпиады» его диплом.



НЕ ПРОСТО МАРИЯ

*Серьёзные увлечения играют
важную роль в становлении
профессионала*



Журнал «BIS Journal — Информационная безопасность банков» продолжает публикации о личностях специалистов, работающих в отрасли. Интересно всё: почему выбрали эту профессию, как обучались её секретам и накапливали опыт, с какими проблемами встречались, и, конечно, что у них за характер, чем интересуются помимо работы. На этот раз наш герой, точнее, героиня — Мария Тюрина, главный специалист отдела информационной безопасности одного из московских банков.

Пленительная восточная мелодия, шуршание старинных афганских украшений, звучание сагатов — маленьких металлических литавр... Девушка движется в необычном танце, сочетающем арабскую грацию, стиль фламенко, тибетскую медитацию. Руки-змеи, украшенные множеством браслетов, мягко трогают воздух, плечи движутся, медленно выводя восьмерку...

Стиль этот называется Tribal. Он родился под вдохновением от танцев Ближнего Востока, Индии, Северной Африки и требует огромной работы с собственным телом, неустанного внимания, способности чувствовать самые тонкие нюансы музыки, чтобы зеркально отражать их в движениях.

Очень красиво! Гибкость, красота, филигранная техника и прекрасный



Наша героиня уверена, что навыки, необходимые для такого танца, служат серьёзным подспорьем в её основной профессии специалиста по информационной безопасности банков

контроль над всем телом. Вы удивитесь, но танцовщица — наша героиня уверена, что навыки, необходимые для такого танца, служат серьёзным подспорьем в её основной профессии специалиста по информационной безопасности банков. Способность обрабатывать большие потоки информации, собирать полную картину из разных источников, концентрироваться на главном, не опуская при этом ни одной мелочи — без этих качеств невозможно обойтись ни в сложных танцах, ни при решении профессиональных задач.

ДОЧЬ ОФИЦЕРА УВЛЕКАЛАСЬ МАТЕМАТИКОЙ

Город Тейково Ивановской области известен тем, что неподалёку базируются ракетные войска стратегического назначения — РВСН. Тут дислоцированы межконтинентальные баллистические ракеты, в том числе «Тополь-М» и «Ярс» и тут же, в военном городке, провела детство Мария Тюрина.

В школе она всерьёз увлеклась математикой, занималась в кружке программирования, а поступить все же хотела в лётное училище — «на пилота». Девушек, к сожалению, туда не брали, поэтому выбирала профессию, связанную с любимыми компьютерными технологиями. Увидела в списке — «Комплексная защита информации», и загорелась. Свою роль сыграла, конечно, и престижность специальности: огромный конкурс, высокие проходные баллы... Это был вызов.

ПЕРВОПРОХОДЦЫ СО СТУДЕНЧЕСКОЙ СКАМЬИ

Владимирский государственный политехнический университет сдался без боя (то ли баллистических ракет испу-

гался, то ли Машиной золотой медали): вместо вступительных экзаменов она в один день решила десять задач по математике, пять по физике, прошла собеседование и... поступила.

Специальность была новой, набор на неё — первым. Порой чувствовалось, что преподаватели «тренируются» на студентах, обкатывают методики, пособия и учебные курсы. И хоть экзаменаторы не взыскивали слишком строго (издержки новизны делили поровну), учиться было нелегко. До диплома дошла ровно половина потока. Любопытно, что трудностей не выдержали в основном мальчишки.

Читать лекции и вести семинары часто приглашали преподавателей-практиков — профессионалов информационной безопасности. В те времена во Владимире их было немного. Приходили служащие государственных органов, включая сотрудников ФСБ России, работники аттестационных центров ФСТЭК, юристы, на опыте знавшие правовую специфику профессии.

Некоторые аспекты информационных технологий увлекали по-настоящему: вычислительные сети как отдельный предмет, базы данных... Преподаватели хорошо разбирались в своих темах, учили реальным полезным вещам, полученные знания и сегодня помогают в работе.

ДИПЛОМ КАК ПОДАРОК... УНИВЕРСИТЕТУ

Учебную практику четвертого курса Мария проходила во Владимирском филиале «Ростелекома». Директор по информационной безопасности был по-настоящему увлечён своим делом и хотел увлечь и практикантов. Делал акцент на технических средствах,



с удовольствием показывал резервные источники питания, дизельные генераторы, пожарную сигнализацию.

Заодно он потряс студентов и виртуозной игрой в Ragnarok — многопользовательскую онлайн-игру. Про онлайн-игры Мария вспоминает с особым чувством: студенты увлекались ими страстно и чуть ли не поголовно, что явно отвлекало от добросовестной учёбы. Однако эти игры воспитывали ценные качества: умение продумывать деловую логику, распределять задачи по приоритетам, ощущать и планировать время. Ничто так не помогало понять принципы управления людьми, как сбор клана на захват замка или на охоту за эпичным монстром...

Но игры играми, а на практике для Марии удачно нашли задание по специальности. А именно разработку системы информационного оповещения пользователей интернета об опасности фишинговых сайтов. Понятие фишинга оказалось для Марии новым, но разобралась, что потом много раз пригодилось.

Преддипломную практику проходила на своей кафедре информационной безопасности. «Первопроходцам» поставили задачу обобщить учебный опыт для тех, кто приходит им на смену. Дипломной работой стал лабораторный комплекс, включающий курс лекций, описание лабораторных работ и программу-презентацию лабораторных работ.

ЗАЩИТА ПРОЕКТА «НА ДЕНЬГИ»

Университет, как и среднюю школу, Мария Тюрина окончила с отличием. Но, учитывая молодость отрасли, устроиться на работу по специальности было всё равно нелегко. Марии повезло, ее взяли в ООО «Банковские системы и серви-

сы — Владимир» специалистом по разработке и тестированию ПО. Компания занималась разработкой программного комплекса «АС София-ВМС» для Волго-Вятского отделения Сбербанка России. Довелось тестировать итог работы коллег — программное обеспечение внутренней автоматизированной банковской системы. Не клиентских дистанционных сервисов, а рабочих мест менеджеров, работающих с клиентами, корпоративный электронный документооборот, постепенно вытеснявший бумажный.

Заказчик составил подробнейшее техническое задание на десятки страниц — огромный труд. Коллеги Марии всё сделали в соответствии с заданием, а потом вместе проводили тестирование на корректную работу.

Сдавать программный продукт ездили в Нижний Новгород. Заказчик задавал каверзные вопросы, указывал на недочеты, угрожал понизить стоимость работ. Процедура напомнила защиту диплома, только «ценой вопроса» оказывалась не оценка, а репутация компании и живые деньги. Всё кончилось хорошо, а Мария приобрела отличный

опыт, не простой, но тем более полезный. Таким образом довелось участвовать в выполнении ряда ответственных проектов.

ПЕРВЫЙ БАНК

Что вначале было в новинку, то, после освоения, стало казаться рутиной. Хотелось новых профессиональных горизонтов, и Мария начала заниматься программированием web-приложений на C# с базой данных (MySQL). Ощутила силы работать самостоятельно и ушла во фриланс.

Одним из заказчиков оказался руководитель подразделения информационной безопасности ООО КБ «АйМаниБанк». Он искал исполнителя своего нового замысла внедрить систему автоматической регистрации пользователей. Нужно было создать удобную, надёжную и хорошо защищённую систему, которая на основании вводимых персональных данных (ФИО) и назначаемой роли автоматически создаёт учётную запись в банковской системе. Формирует адрес электронной почты, предоставляет доступ к различным информационным системам банка в соответствии с указанной ролью сотрудника и т.п.

Около двух лет ушло у Марии на создание и внедрение такого ПО. Внедрение первого релиза системы было совершено через полгода после начала работы. Ещё полтора года его улуч-

Еще одна сфера ответственности — работа с сотрудниками банка и клиентами, информирование их об актуальных угрозах, правилах информационной безопасности

шали и дополняли программными решениями для сбора и анализа логов работы сотрудников банка в интернете. Когда руководитель подразделения уходил на новое место работы, он пригласил и рекомендовал её как надёжного и квалифицированного специалиста в штат.

ВСЕ ВПЕРЕДИ!

Впечатления от новой работы оказались чудесными: заниматься приходилось многим, всё было интересно. Никакой рутины, зато опыт набирался «тоннами».

В сфере ответственности главного специалиста не столь многочисленного отдела ИБ сосредоточены практически все направления: работа с криптографическими и другими средствами защиты информации, контроль корпоративной электронной почты и электронного документооборота в целом, съёмных устройств, комплаенс и многое другое. А также «гуманитарные» вопросы — фишинг, социальная инженерия, прямые мошенничества.

Еще одна сфера ответственности — работа с сотрудниками банка и клиентами, информирование их об актуальных угрозах, правилах информационной безопасности. Приятно видеть результаты, когда «аудитория» с интересом и быстро учится, начинает распознавать угрозы, присылает сообщения о них.

ОТ РЕДАКЦИИ

Многообразие жизни весьма поучительно. Разве до встречи с Марией вы знали, что ИБ и танцы — близнецы-братья? Что их сближает умение понимать сложную технику и владеть ей в совершенстве? Или то, что исполнителя, как и злоумышленника, определяют по инструментарию и «почерку» — нюансам стиля, базовому ПО, осанке, манере двигаться? И наконец, что там и там, как в сообщающихся сосудах, используются зачастую одни и те же человеческие способности и качества?

Несмотря на видимые результаты своей деятельности, Мария не спешит называть себя полностью состоявшимся профессионалом. Говорит, нужно ещё осваивать очень многое, развивать уже имеющиеся навыки и компетенции, осваивать практические вещи: новые средства защиты, способы поиска и эксплуатации различных уязвимостей в программном обеспечении и сетевых протоколах, способы защиты от хакерских атак... Цели профессионального роста, в первую очередь, — повышение квалификации, получение новых знаний, расширение опыта.

СУДЬБОНОСНОЕ УВЛЕЧЕНИЕ

Мария — человек разносторонний. И увлечения у нее не только в профессиональной сфере. Со школы она любит физкультуру и гимнастику, а когда учеба закончилась, нашла себя в пластике. Ее страсть — Tribal Style, сложный «микс» восточных танцев.

Восточные танцы были выбраны не случайно: как своего рода отрицание бывшего увлечения пауэрлифтингом. Силовые упражнения приучали к рационально простому, механическому движению, а танец, напротив, покорял сложностью, сопоставимой с компьютерной игрой-квестом. Овладеть таким мастерством стало очередным вызовом.

Тут важно понимать, что речь идет о танцевальной системе, своеобразном

языке, состоящем из набора движений и знаков, которые танцовщицы подают друг другу на сцене. Восхитительная прелесть этого действия в том, что несколько совершенно незнакомых между собой людей, зная этот язык, могут без предварительного сговора и репетиций станцевать полноценный танец, красиво и синхронно, создавая его на лету здесь и сейчас.

Например, один из принципов этой системы называется flock of birds — «стая птичек» или «рыбок». Он означает, что танцоры в группе взаимодействуют между собой как одно целое. Если лидер поворачивается на несколько градусов, то все остальные поворачиваются за ним ровно на столько же.

* * *

Участие в таком действе отлично развивает внимание, умение быстро реагировать и принимать решения. Ведь нужно следить не только за лидером, а еще и за собственным лицом, за техникой исполнения, а если сам стал лидером, то и за музыкальными фразами, акцентами, чтобы вовремя вкинуть нужное движение, дать знак группе. Само собой — это неповторимый опыт командной работы, и такие принципы взаимодействия как нельзя кстати и для применения в рабочем кабинете.

Которые, на минуточку, развить и отточить, занимаясь танцами, гораздо проще и быстрее, чем непосредственно в профессии ИБ. Так что советуем, последуйте примеру Марии, займитесь Tribal Style.

P.S. Общение обогащает! Ждем от вас рассказов или информации о коллегах, чьи увлечения расширяют представления о профессии специалиста информационной безопасности или представляют ее в неожиданном ракурсе.



ОНИ КОВАЛИ ПОБЕДУ

**О выдающемся советском
криптоаналитике С. С. Толстом**

2 сентября 1945 года закончилась Вторая мировая война. Финальную точку в ней поставило вступление в войну против Японии СССР, стремительное наступление советских войск вынудило японское руководство капитулировать. Огромную роль в советско-японском противостоянии в годы Великой Отечественной войны сыграл выдающийся отечественный криптограф Сергей Семенович Толстой (1899–1945).

ОГНЕВАЯ МОЛОДОСТЬ

Он родился 5 октября (22 сентября) 1899 года в селе Старо-Захаркино Петровского уезда Саратовской губернии в семье служащего в Саратовском имении графов Толстых. Когда Сергею было 8 лет, семья с шестью детьми осталась без отца, а в 1916 году и без матери. В 1913 году С. С. Толстой окончил сельское училище и поступил на службу письмоводителем в Старо-Захаркинское волостное управление, а затем перешел на службу в штаб одной из воинских частей. С декабря 1917 года по август 1919 года прини-

мал активное участие в организации Советов солдатских и крестьянских депутатов в родном селе. Организовал там волостной Комитет РКП(б), несколько раз участвовал в подавлении кулацких восстаний. В августе 1919 года был мобилизован в Красную Армию и в мае 1920 года, будучи писарем Штаба 34-й дивизии Красной Армии, впервые познакомился с шифровой работой. В сентябре того же года был откомандирован в распоряжение специального отдела Реввоенсовета Республики. В 1921 году окончил специальные курсы ВЧК. С 1922 года работал в Специальном отделе ГПУ-ОГПУ.

НЕОЖИДАННЫЙ ТАЛАНТ

В Спецотделе проявил себя талантливым специалистом. Его авторитет среди сотрудников Спецслужбы постепенно стал огромным. Талант С. С. Толстого особенно раскрылся в трудные предвоенные годы и годы Великой Отечественной войны. Находясь в Москве, С. С. Толстой оказывал действенную помощь испанским республиканцам

в борьбе с генералом Франко, дешифруя перехваченные криптограммы фашистов. В 1940 году старший лейтенант госбезопасности Толстой, в связи с успешным завершением финской кампании, был награжден первым своим орденом — «Знак Почёта». В течение многих лет был ведущим специалистом в службе и внес большой вклад в развитие отечественной криптографии. Им лично и под его руководством было раскрыто много сложных шифров иностранных государств. Созданная им методика раскрытия ряда систем ручного и машинного шифрования имела большое практическое значение.

В ЯПОНСКОМ ОТДЕЛЕ

В предвоенные годы С. С. Толстой возглавлял японский отдел дешифровой службы НКВД. Задача по дешифрованию японской переписки была очень непростой. Сам язык, письменность, азбука катакана, ее телеграфный код Морзе — все это было так необычно, что пришлось тщательно изучать написание и название знаков азбуки катакана, комбинаций их



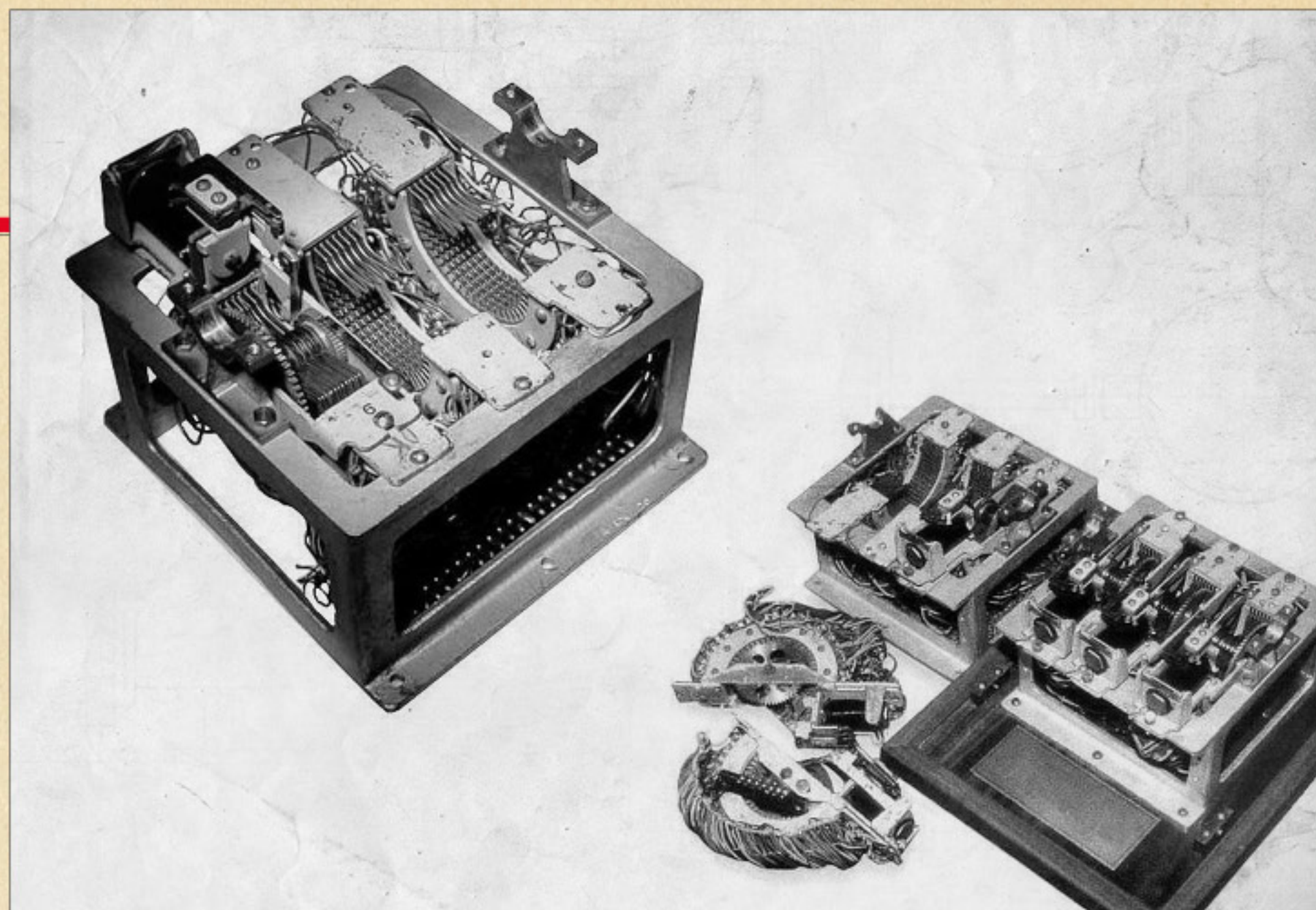
Геннадий ЕМЕЛЬЯНОВ
член-корреспондент
Академии Криптографии РФ



Дмитрий ЛАРИН
кандидат технических наук



Советский криптоаналитик
Сергей Семенович Толстой (1899–1945)



Японская «пурпурная машина»

телеграфных посылок, понимать, как передается текст: латынью или катаканой — для его правильной записи и т.д. Однако все трудности были преодолены, и группа С.С. Толстого приступила к систематическому чтению японской шифрпереписки. Одним из самых крупных успехов накануне войны было дешифрование группой специалистов во главе с Толстым японских шифрмашин, известных под названиями, данными им американцами, — «оранжевая», «красная» и «пурпурная» [Кузьмин, 1998–1, с. 85], [Анин, 1996, с. 280]. Важное место среди японских шифров принадлежит дисковой «пурпурной машине». Японцы ещё в апреле 1937 года стали испытывать её на некоторых дипломатических линиях связи. Массовое же применение машины началось с февраля 1939 года. Этим шифратором закрывалась наиболее секретная переписка японского МИДа со своими дипломатическими органами в Европе, Азии и Америке, в частности, она применялась посольствами в таких важных пунктах, как Москва, Берлин, Рим, Стокгольм, Мадрид, Берн, Виши, Анкара и др. [Ландер, 2007], [en.wikipedia], [Kahn, 1967].

ПУРПУРНАЯ МАШИНА

Японская «пурпурная машина» — оригинальная по тому времени система шифрования, её описание, в частности, можно найти в главе 2 книги [Бу-

тырский, 2012]. К её дешифрованию было привлечено значительное количество опытных криптоаналитиков. В тот период все процессы по исследованию закономерностей шифртекста, различного рода статистические расчеты и другие работы осуществлялись, как правило, вручную, что удлиняло сроки взлома шифратора. Тем не менее, благодаря настойчивым усилиям наших криптографов, разработка была в конце 1941 года успешно завершена, что по тому времени явилось большим достижением и показало возможность раскрытия машинных шифрсистем. Как уже отмечалось выше, эта работа была выполнена группой криптографов под руководством С.С. Толстого. При этом отметим, что «пурпурная машина» не оправдала надежд японского руководства, помимо СССР её читали в США, Великобритании, Нидерландах, а также немецкие союзники Токио [Анин, 1996], [Бутырский, 2012], [Кошкин, 1989], [Кузьмин, 1998], [Ландер, 2007], [Kahn, 1967], [topcatalog].

ВКЛАД В ПОБЕДУ ПОД МОСКВОЙ

Отметим, что успешные результаты по чтению зашифрованной японской дипломатической переписки позволили сделать вывод о том, что Япония не намерена начинать военные действия против СССР. Это дало возможность перебросить большое количество сил на советско-германский фронт. В частности, с Дальнего Востока и из Сиби-

ри были переброшены 15 стрелковых и 3 кавалерийские дивизии, 1700 танков и 1500 самолетов. Эти силы были вовремя переброшены на запад, к Москве. Они оказали существенную помощь в обороне столицы и последовавшем контрнаступлении под Москвой. Как известно, сражение под Москвой стало первым крупным поражением немецкой армии в ходе Второй мировой войны.

Напряженный труд работников дешифровальной службы в годы войны был высоко отмечен партией и правительством. В газете «Правда» № 94 (8865) от 4 апреля 1942 года был опубликован Указ Президиума Верховного Совета СССР «О награждении работников НКВД Союза ССР за образцовое выполнение заданий Правительства» от 3 апреля 1942 года. 54 специалиста были награждены орденами и медалями Советского Союза. В том числе Орденом Ленина награждены два капитана государственной безопасности Б.А. Аронский¹ и С.С. Толстой, орденом Трудового Красного Знамени 6 человек, орденами Красной Звезды и «Знаком почета» — 13 человек и медалями «За трудовую доблесть» и «За трудовое отличие» — еще 33 человека. Так советское правительство оценило вклад дешифровальщиков в победу под Москвой [Кузьмин, 1998, с. 83].

¹ О криптографической деятельности Бориса Алексеевича Аронского мы подробно расскажем в одном из следующих номеров журнала.

ВОЕННАЯ И ДИПЛОМАТИЧЕСКАЯ ШИФРПЕРЕПИСКА

В дальнейшем С. С. Толстой и его сотрудники продолжали дешифрование японской шифрпереписки, что позволяло советскому руководству быть в курсе позиции Японии относительно нападения на СССР. Напомним, что даже в 1944 году «горячие головы» из командования Квантунской армии хотели напасть на СССР, но их постоянно одергивали из Токио, вся эта информация, благодаря работе советских дешифровальщиков под руководством С. С. Толстого, была доступна нашим политическим и военным руководителям.

В СССР в период советско-японского противостояния наряду с дешифрованием японской военной переписки (этим занимались в основном армейские и флотские криптографы), серьезное значение имело систематическое чтение дипломатических шифрматериалов. Раскрытие дипломатических шифров Японии и ряда ее союзников было возложено на дешифровальную службу НКВД, хотя и она работала с военной перепиской [Бутырский, 2012].

В шифрпереписке между Токио и его посольствами не раз обсуждались военные и политические планы нашего основного противника — Германии

Если военная переписка освещала ход военных действий на определенных участках фронта и позволяла делать выводы главным образом о тактических действиях противника, то систематическое чтение дипломатической шифрпереписки, ведущейся на государственном уровне, было призвано помогать руководителям СССР, дипломатам, советской разведке раскрывать стратегические замыслы и тайные планы Японии в отношении нашей страны в условиях войны. При этом отметим, что в шифрпереписке между Токио и его посольствами не раз обсуждались военные и политические планы нашего основного противника — Германии. Во многих шифртелеграммах содержалась весьма подробная информация о состоянии немецкой армии и оборонной промышленности, а также важная политическая информация.

Полезную информацию дешифровальная служба давала о разведывательной деятельности японских дипломатов и военных атташе против Советского Союза и других стран. Телеграммы содержали план создания японцами информационной сети в Европе. Все эти криптограммы были прочитаны. Определенный интерес представляла также экономическая информация, из которой, в частности, хорошо раскрывалась позиция Японии при подготовке и проведении переговоров с Советским Союзом по спорным рыболовным и концессионным вопросам. Как это следует из дешифрованной переписки, при ведении экономических переговоров японская сторона руководствовалась прежде всего политическими соображениями, исходила из обстановки на советско-германском фронте. Так, в первый период войны Япония в своих требованиях к СССР стремилась занимать жесткую линию, однако по мере ухудшения положения немцев на советско-германском фронте её позиция смягчалась, и одновременно усиливалось стремление склонить СССР к продолжению пакта о нейтралитете. Читая японскую переписку, представлялось возможным получать много важной информации непосредственно по Германии. Японские дипломаты и военные атташе, следя за положением Германии и изучая её военно-промышленный потенциал, систематически передавали секретные сведения по немецкой армии, военно-воздушным и военно-морским силам, данные о новых образцах оружия, работе военной промышленности, людских ресурсах и др. И конечно же важнейшую роль играла информация о намерениях Японии в отношении СССР.



Вид Токио, 1930 гг.



Японский военный атташе в Стокгольме генерал-майор Макото Онодэра во время посещения немецкой береговой батареи «Фьелль»

ЖЕНА НАДЕЖНЕЕ МАШИНЫ

В период Великой Отечественной войны наша дешифровальная служба читала в значительном объёме шифрпереписку японской армии и военных атташе (напомним, что во всём мире данная должность фактически является названием легального агента военной разведки). Япония имела весьма разветвлённые сети шифрованной связи в большинстве стран мира. Связь велась очень активно, а сведения, проходившие по этим каналам связи, представляли большой интерес для советского руководства. Япония во время войны применяла довольно большое количество шифрсистем, различных по своему построению и стойкости. Использовались шифры замены и перестановок, коды без перешифровок и с перешифровками, а также шифрмашин. При этом имелись шифрсистемы для циркулярной, зональной и индивидуальной связи. Для зашифрования текста телеграмм широко практиковалось одновременное применение нескольких кодов. Так, в 1941 году японская дипломатия использовала 19 различных кодов, в 1942 году — 20, в 1943 году — 19, в 1944 году — 10, в 1945 — 9. Сроки действия шифров исчислялись годами, месяцами и даже днями [Бутырский, 2012].

Интересно отметить следующий факт. Назначенный в октябре 1940 года японским военным атташе в Швеции полковник Макото Онодэра (к концу войны дослужился на этом посту до звания генерала) не доверял имеющимся в распоряжении японской мис-

сии шифрмашин. Ещё с 1938 года, когда Онодэра работал атташе в Риге (Латвия), шифрованием сообщений занималась его супруга Юрико. Она была квалифицированным криптографом и тщательно соблюдала правила конспирации при работе с шифрами. Вот что по этому поводу она позже писала в своих мемуарах: «... научилась аккуратно обращаться с шифрблочком и незаметно маскировать его в случае нахождения вне резиденции в складках кимоно» [Забелин, 2008]. Переехав вместе с мужем в Швецию, она продолжала пользоваться «трудоемким ручным способом кодирования секретных сообщений между резидентом японской военной разведки и Генеральным штабом. То обстоятельство, что г-жа Онодэра не пользовалась имеющейся в её распоряжении шифровальной машиной... уберегло их секретную корреспонденцию от дешифровки союзническими криптоаналитиками» [Забелин, 2008].

ВНУШИТЕЛЬНАЯ СТАТИСТИКА

Также информацию о намерениях и планах Японии советское руководство получало не только из японской шифрпереписки, но и из дешифрованных немецких и итальянских телеграмм. Немцы и итальянцы активно обсуждали позицию японского руководства

по тем или иным вопросам, часто эта информация становилась достоянием наших криптоаналитиков. Анализ перехваченных и дешифрованных нашими спецслужбами радиogramм Японии и ее союзников свидетельствует, что советским криптоаналитикам удавалось прочитывать их содержание и своевременно докладывать эту информацию советскому руководству [Бутырский, 2012]. По всем системам шифров за годы войны было перехвачено 132 113 телеграмм, из них дешифровано 97 446. Японская переписка почти полностью контролировалась.

ТЕЛЕГРАММЫ, ТЕЛЕГРАММЫ...

Приведем здесь тексты ряда японских телеграмм, дешифрованных советскими криптографами во главе с С. С. Толстым накануне и во время Великой Отечественной войны.

Вот, например, фрагмент из телеграммы генерального консула Японии в Вене Ямадзи японскому послу в Москве о позиции Японии в отношении Советского Союза, отправленной 30 августа 1939 года:

Я телеграфировал в Токио за № 76.

Дополнительно телеграфирую следующее:

1. Курс в отношении СССР. Для обеспечения безопасности империи на всегда необходимо, я полагаю, когда нами будет достигнута в должной степени государственная мощь, в один прекрасный момент пойти на войну с Советским Союзом и захватить в свои руки его территории на Дальнем Востоке. Однако в условиях новой ситуации как временная линия по отношению к СССР, по моему мнению, следует держаться установленных позиций, вместе с тем связывать действия СССР и поступать не спеша. Не подлежит сомнению, что позиции СССР на Дальнем Востоке в результа-

По всем системам шифров за годы войны было перехвачено 132 113 телеграмм, из них дешифровано 97 446



Европа перед Второй мировой войной. Немецкая агрессия 1936–1939 гг.

те германо-советского договора значительно усилились и необходимо с предельным вниманием отнестись к тому, какую позицию займёт СССР по отношению к нам, пользуясь своим новым положением. Но не надо опасаться, что так или иначе его внешняя политика по отношению к Японии примет более позитивный характер. Не исключено, что, начав с вопроса о концессиях, границах и пакте о ненападении, СССР попытается точно определить сферы влияния в Азии. Конечно, в этом случае, дабы сделать свои позиции выгоднее, СССР не покусится на различные манипуляции.

Мои мысли на этот случай таковы: а) для нашей империи, устремляющейся к реализации своих идеалов, было бы очень хорошо, если бы она смогла заставить теперь СССР отказаться от политики помощи Чан Кайши и большевизации Дальнего Востока и если бы удалось таким образом урегулировать отношения между обеими странами. Поэтому, если СССР, как я говорил выше, займёт позицию на сближение с нами, нам, сохраняя со своей стороны позицию полного нейтралитета, следует искусно втянуть его в переговоры, а когда положение достаточно определится, то ничто не мешает заключить

даже и пакт о ненападении. Но, конечно, в любых обстоятельствах надо обращать максимальное внимание на то, чтобы престиж империи и её принципиальные позиции не были ущемлены. Ямадзи. ЦА ФСК России [Органы, 1995, том 1, книга 1].

ТЕЛЕГРАММА ЯПОНСКОГО ПОСЛА В МОСКВЕ ЯПОНСКОМУ ПОСЛАНИКУ В СОФИИ

9 июня 1941 г.

Усиленно циркулирующие слухи о том, что Германия нападёт на Советский Союз, а в особенности информация, поступающая из Германии, Венгрии,

Ценнейшая информация была получена из дешифрованных сообщений представителей союзников Германии в столице Финляндии Хельсинки

Румынии и Болгарии, заставляют думать, что приблизился момент этого выступления.

Я думаю, что каким бы превосходством ни обладала германская армия, победить или же разгромить Советский Союз в течение 2–3 месяцев, как об этом циркулируют слухи, будет невозможно. Более того, не исключена даже возможность того, что Германия окажется в состоянии затяжной войны.

Обстановка в Москве весьма спокойна, незаметны также и признаки подготовки к войне, а именно: мероприятия ПВО, сокращение количества такси и прочее. 24 мая я спросил об этом у Молотова. Он ответил, что в настоящее время между Германией и Советским Союзом не имеется трений, могущих повлечь к войне, но если возникнет конфликт, то он считает своим долгом разрешить его мирным путем. Кроме того, позавчера, 7-го числа, германский посол в беседе со мной сказал, что от правительства по этому вопросу никаких сообщений нет, что нет признаков подготовки к войне со стороны Советского Союза, который, должно быть, знает о существующей щекотливой ситуации, а кроме того, Советский Союз аккуратно выполняет обещания, данные Германией, поэтому трудно изыскать причины для нападения на Советский Союз.

Татекава (*Иосицугу — посол Японии в СССР с октября 1940 г. по март 1942 г. — авт.*). ЦА ФСРК России [Органы, 1995, том. 1, книга 2].

В начале июня 1941 года нашими спецслужбами были дешифрованы телеграммы японского представителя в Кенигсберге японскому послу в Москве о военных приготовлениях немцев в Восточной Пруссии.

ТЕЛЕГРАММА ИЗ КЕНИГСБЕРГА ЯПОНСКОМУ ПОСЛУ В МОСКВЕ

9 мая 1941 г.

Последнее время ежедневно между Берлином и Кенигсбергом проходит в северном направлении около 10 военных железнодорожных составов, вагоны очень больших размеров с французских железных дорог. В здешних военных кругах считают, что в настоящее время в Восточной Пруссии сконцентрированы крупные военные силы, по количеству не уступающие военным силам в Люблинском районе, и что в июне германо-советские отношения должны будут как-то определиться. Отдано распоряжение о том, чтобы большинство немецких офицеров к концу мая в обязательном порядке овладело русским языком хотя бы в рамках чтения.

Сугихара. ЦА ФСРК России [Органы, 1995, том. 1, книга 2].

В первой из них сообщалось:

«В течение последней недели из Мемельского порта (*ныне город Клайпеда на территории Литвы, в описываемое время принадлежал Германии — авт.*) была направлена в Финляндию часть расположенных в Мемельской области войск... в этом районе происходит их концентрация... пассажирский поезд, который вышел из Берлина утром 29 мая и прибыл сюда в тот же день вечером, на пути разминуслся с 38 порожними воинскими составами. Военные перевозки по линии Познань — Варшава проходят более оживленно, чем в этом районе... 30 мая мною замечено, что между всеми пунктами восточнее Кенигсберга проведен телефон... Все это наводит на мысль о начале войны» [Сыромятников, 2001, с. 21].

10 июня 1941 года из данного источника была получена следующая информация:

ТЕЛЕГРАММА ИЗ КЕНИГСБЕРГА ЯПОНСКОМУ ПОСЛУ В МОСКВЕ

10 июня 1941 г.

Телеграфировал в Токио за № 15.

1. 5 июня через Кенигсберг прошли в восточном направлении две дивизии легких танков, а 7 июня — несколько мотомехдивизий.

2. Перевозки по железным дорогам по-прежнему проходят оживленно. Выехав утром 9-го числа из Берлина в Кенигсберг, мы по пути перегнали шедшие в восточном направлении 17 воинских железнодорожных составов (12 составов с мотомехчастями, 3 — с танками, 1 — с полевой артиллерией и 1 — с санитарными частями). На восточных концах важнейших мостов установлены тяжёлые пулеметы.

3. 6 июня к здешнему военному штабу дополнительно прикомандировано из Берлина 25 офицеров генштаба.

4. Говорят, что численность здешнего гарнизона составляет 300 000 человек. Все воинские части в этом районе имеют при себе противогазы.

Телеграфировал в Рим, Берлин, Москву [Органы, 1995, том. 1, книга 2], [Сыромятников, 2001, с. 29–30].

Ценнейшая информация была получена из дешифрованных сообщений представителей союзников Германии в столице Финляндии Хельсинки. Из переписки посольства Японии:

ТЕЛЕГРАММА ИЗ ХЕЛЬСИНКИ ЯПОНСКОМУ ПОСЛУ В МОСКВЕ

18 июня 1941 г.

В смысле вооружений Финляндия и после прошлогодней войны с Советским Союзом продолжает всё время поддерживать обстановку военного времени. В особенности усиливаются оборонительные сооружения на восточной границе. Хотя до настоящего времени официальных сообщений не было, однако недавно стала проводиться вновь фак-

тическая всеобщая мобилизация. 15-го числа было призвано в воинские части только по одному Хельсинки 10 000 человек. Призыв продолжается. Далее, идёт призыв женщин в санитарные и продовольственно-питательные отряды (в равной степени призываются также и женщины-уборщицы и прочий обслуживающий персонал правительственных учреждений). На важных участках города установлена зенитная артиллерия. Молодежь в секретном порядке вступает в германскую армию и, по-видимому, мечтая о проведении карательной войны против Советского Союза, надеется на возвращение утерянных территорий. Резко сократилось количество рабочих, в городе не хватает такси.

Сакая. ЦА ФСБ России. [Органы, 1995, том. 1, книга 2].

ТЕЛЕГРАММА ИЗ ХЕЛЬСИНКИ В МИНИСТЕРСТВО ИНОСТРАННЫХ ДЕЛ ЯПОНИИ

19 июня 1941 г.

Учитывая обстановку, существующую здесь, я сжёг нижеследующие секретные документы:

1. Все военно-морские шифры, шифры «Канада», «Германия», «Канаэ», «Зеландия», «Аляска» (очевидно, условные наименования кодовых книг — авт.).

2. Все телеграммы и секретные отношения, за исключением телеграмм и отношений за 1941 г.

3. Все секретные протоколы.

Если возникнет чрезвычайная обстановка, то я оставлю только шифры «Бельгия», «Перу», «Колумбия» и «Куба», а остальное сожгу.

Сакая. ЦА ФСБ России [Органы, 1995, том. 1, книга 2], [Сыромятников, 2001, с. 28].

Важная информация поступала из столицы Румынии Бухареста. Так, за два дня до нападения немцев была дешифрована телеграмма, отправленная в Токио послом Японии:

ТЕЛЕГРАММА ИЗ БУХАРЕСТА ЯПОНСКОМУ ПОСЛУ В МОСКВЕ 20 июня 1941 г.

Телеграфировал в Токио.

Лично главе учреждения. Совершенно секретно.

Утром 20 июня германский посланник сказал мне доверительно следующее:

«Обстановка вошла в решающую фазу развития. Германия полностью завершила подготовку от Северной Финляндии и до южной части Черного моря, закончила формирование

и вооружение по штатам военного времени 154 дивизий, предназначенных для нападения на СССР, и уверена в молниеносной победе. Румыния также по мере возможности ведёт подготовку к тому, чтобы можно было сразу выступить (на стороне Германии — авт.). Я лично вполне доволен».

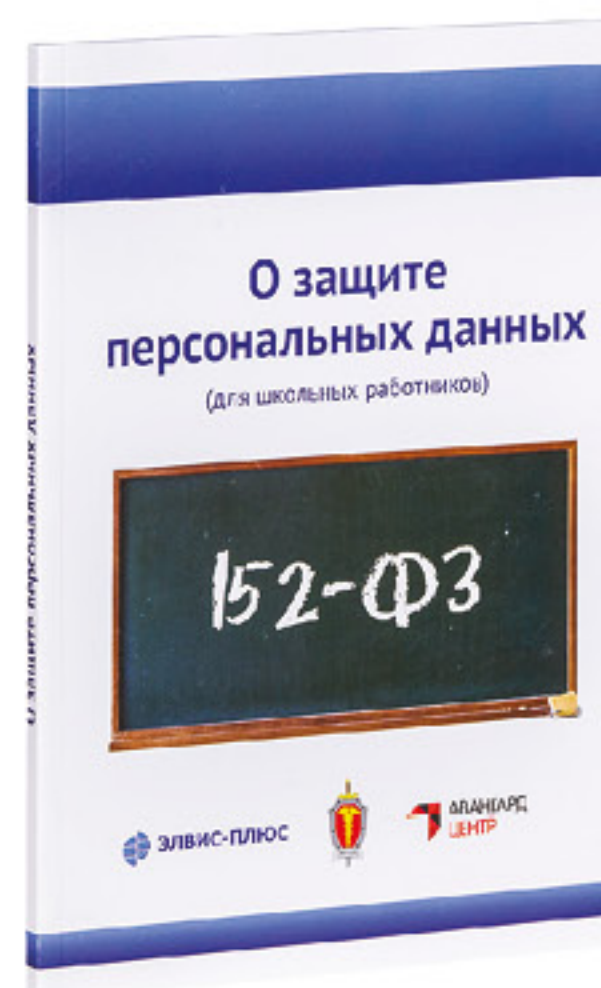
Цуцуи. ЦА ФСБ России [Органы, 1995, том. 1, книга 2], [Сыромятников, 2001, с. 22, 28].

(Окончание в следующем номере)

ЛИТЕРАТУРА

1. [Анин, 1996] Анин Б. А., Петрович А. И. Радиошпионаж. М.: «Международные отношения», 1996.
2. [Бутырский, 2012] Бутырский Л. С., Ларин Д. А., Шанкин Г. П. Криптографический фронт Великой Отечественной. Монография. М.: Гелиос АРВ, 2012. 2 изд. исправл. и дополн. М. 2013.
3. [Забелин, 2008] Забелин А. Центр японского шпионажа в Скандинавии // Независимое военное обозрение № 6, 2008, с. 7.
4. [Кошкин, 1989] Кошкин А. А. Крах стратегии «спелой хурмы». Военная политика Японии в отношении СССР 1931–1945 гг. М.: «Мысль», 1989.
5. [Кузьмин, 1998] Кузьмин Л. А. Не забывать своих героев // Защита информации. Конфидент № 1, 1998, с. 83–85.
6. [Ландер, 2007] Ландер И. И. Негласные войны. История специальных служб 1919–1945. Одесса, «Друк» 2007. <http://www.lander.odessa.ua>
7. [Органы, 1995] Органы государственной безопасности СССР в Великой Отечественной войне 1941–1945. Сборник документов. М.: «Русь» 1995.
8. [Соболева, 2002] Соболева Т. А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002.
9. [Сыромятников, 2001] Сыромятников Б. А было ли нападение внезапным? // Сигары Шееле для «Барона Дризена» М.: «Издательский дом Гелеос», 2001, с. 17–34.
10. [Черевко, 2010] Черевко К. Е. Военные тайны XX века — Серп и молот против самурайского меча. М.: Российская Академия наук. Институт российской истории // www.modernlib.ru, www.fb2book.com. 21.11.2010.
11. [Энциклопедия, 2004] Энциклопедия секретных служб России. М.: Астрель, 2004.
12. [en.wikipedia] <http://en.wikipedia.org>
13. [Kahn, 1967] Kahn D. The codebreakers. N- Y: Macmillan Publ. Co., 1967.
14. [topcatalog] www.topcatalog.com.ua/news/322245.html
15. [vif2ne] <http://vif2ne.ru/forum/0/archive/1788/178855.htm>

Издательство Медиа Группы «Авангард»



Лучшие книги по ИБ
теперь можно купить онлайн:

books.ib-bank.ru

Если ночью кто-то прикоснулся косматой
лапой, надо спросить: «К добру или к худу?»
Народная примета

МЕНЯ ТЕРЗАЮТ СМУТНЫЕ СОМНЕНИЯ...

О новом законе о ККТ, тайнах и стенаниях о Большом Брате

Вот и наступила осень, а вместе с ней вступил в силу и новый закон о контрольно-кассовой технике. Уже и первые операторы фискальных данных появились, а все равно — страшно! Да, все новое — страшно! И страшно это потому, что неизвестно. Страшно входить в темную комнату, потому что не знаешь, что тебя там ждет, страшно переходить неизвестную реку в брод, потому что не знаешь, как она себя поведет. А тут еще и Интернет не молчит. «А-а-а! — кричат одни, — ввели тотальное слежение за каждой покупкой, начиная от бутылки воды, до квартиры!». Другие, такие как исполнительный директор «Опоры России» Андрей Шубин, им вторят: «Компании беспокоятся за сохранность коммерческой тайны и не хотят передавать данные о продажах по номенклатуре даже государству. Посредник — оператор фискальных данных (ОФД) будет аккумулировать такие данные. Это промежуточное звено увеличивает риск изменения данных или их передачи конкурентам! И вообще, открытость передаваемых данных усиливает риск киберугроз!»

Чтобы страхи развеять, надо больше знать. Больше знать о том, что там, «за горизонтом», чем все это может грозить. Знание — сила! Вот давайте попытаемся взглянуть на эту ситуацию с разных точек зрения, посмотреть, что же все-таки может быть и, наконец, определить: к добру это или к худу. А точек зрения здесь, как минимум, три: с одной стороны, это государево око, мытари в лице налоговых органов, с другой это, конечно мы все с вами вместе взятые покупатели (обыватели) и с третьей стороны, это конечно же продавцы, которые в терминах ФНС России называются налогоплательщиками.

Но, сначала, давайте посмотрим, как все происходит и что здесь нового. Раньше было так: Вы приходите в магазин, делаете покупки, платите и Вам дают бумажный чек. Все, это и есть фискальный документ, который с одной стороны служит Вам оправданием сделанной покупки, а, с другой стороны, служит отправным моментом для определения налогооблагаемой базы для налогоплательщика. Правда, для этого ему надо своевременно сдать ЭКЛЗ — некий накопитель, который и позво-

лит налоговым органам правильно рассчитать налоги. Теперь все так и не так. Появляется дополнительное промежуточное звено — оператор фискальных данных — которое принимает чеки от налогоплательщика в режиме on-line, передает их в налоговые органы и вдобавок еще накапливает их и, с определенной периодичностью, опять же, передает в налоговые органы. Вот это-то новое промежуточное звено и порождает те самые страхи.

СТРАХИ ОБЫВАТЕЛЯ

Больше всего в этой ситуации обывателя смущает то, что, как говорит Андрей Шубин, «все данные о любой его покупке теперь будут сразу направляться в налоговый орган, храниться в его личном деле и могут быть использованы против него через тысячи лет! Спецслужбы теперь будут знать, что он ест, пьет, где бывает и живет, с кем живет, какие есть домашние любимцы, увлечения, настроения, каждый ваш шаг в течении всей вашей жизни». (Ну прямо по Оруэллу!) Так ли это? Нет, не так! Действительно, в недрах информационной системы оператора фискальных данных в течение пяти лет хранится вся информация о всех покупках, сделанных через кассовую технику, подключенную к нему. И в налоговые органы он эту информацию передает. Это так. А вот дальше — не так. Чтобы выбрать из всего этого массива информацию, принадлежащую одному конкретно-

Вопреки растиражированной информации о том, что в каждом кассовом чеке, направляемом в налоговые органы, будут персональные данные покупателя, такого требования в законе нет



му субъекту, эта информация должна быть проиндексирована, то есть привязана к какому-то конкретному идентификатору, который позволяет отличить Васю Пупкина от всех других. Но в чеке такой информации просто нет! Да, там указано, где (в каком магазине), когда, что и сколько куплено, но не указано, кто купил. Вопреки растиражированной информации о том, что в каждом кассовом чеке, направляемом в налоговые органы, будут персональные данные покупателя, такого требования в законе нет. Новый закон предполагает, что в будущем бумажные чеки уйдут в небытие и вся информация будет передаваться в электронном виде на электронную почту покупателя. Впрочем, это дело добровольное и каждый покупатель решает для себя сам — сообщать или не сообщать продавцу свою электронную почту. Да и размещаемый на кассовом чеке абонентский номер либо адрес электронной почты покупателя сами по себе, без идентификационных персональных данных персональными данными не является. И по электронной почте нельзя идентифицировать однозначно покупателя. А если он использует почту своей жены, друга или специально заведенный для этих целей анонимный почтовый ящик? Нет, и по этому признаку отсементировать все покупки, принадлежащие одному покупателю, невозможно. То есть, эти страхи обывателя — беспочвенные, не узнаешь ты о нем что-либо новое, даже перелопатив всю имеющуюся у оператора фискальных данных базу данных.

С другой стороны, покупатель получает возможность всегда проверить пра-

вильность чека и проведенной с его помощью транзакции. Достаточно навести на чек QR-сканер, который есть в любом смартфоне и получить всю исчерпывающую информацию о продавце и совершенной транзакции. Кроме того, покупатель имеет теперь возможность в любой момент получить электронную копию чека, что значительно снижает риск конфликтных ситуаций, возникающих при обмене некачественного товара и отстаивании интересов покупателя в суде.

СТРАХИ НАЛОГОПЛАТЕЛЬЩИКА

Главное, что боится налогоплательщик — потерять бизнес. Действительно, сведения о номенклатуре продаваемых товаров, динамике их продаж, эффективности ценовой политики, объемах продаж — все это может быть предметом маркетинговых исследований и составлять коммерческую тайну и влиять на бизнес. Естественно, что никому не хочется отдавать свои секреты чужому. А тут, у оператора фискальных данных — вся информация, да еще и в режиме on-line! А еще на чеке есть фамилия индивидуального предпринимателя, его ИНН и фамилия кассира, совершившего транзакцию, а это уже персональные данные, защищаемые по закону. Страшно! Так-то оно так, но, ведь и сейчас каждый налогоплательщик обязан сдать ЭКЛЗ, на которой хранится такая же информация, в ЦТО и новый порядок вряд ли что-то страшного добавит, разве что сокращается время получения обобщенной информации, если недобросовестный оператор решит воспользоваться таким случаем. А еще у каждой кассы сей-

час стоит специальная емкость, в которую складываются выбитые чеки (наши покупатели — народ странный, они почему-то не любят брать с собой чеки и бросают их рядом с кассой). Не думаю, что эти чеки подвергаются какому-то специальному способу утилизации, их просто выкидывают в мусорный бак. В этом случае тому, кто хочет получить определенную маркетинговую информацию, достаточно собрать эти чеки и проанализировать. И не надо лезть в информационную систему оператора фискальных данных. Ну, положим, что оператор фискальных данных все-таки решил кому-то «слить» такую информацию. Техническая возможность у него есть. Однако, такой слив грозит ему потерей бизнеса. Ведь ему ФНС России дает специальное разрешение на обработку фискальных данных, проведя перед этим особую проверку, удостоверившись, что информация защищается, что к ней нет доступа посторонних, что она правильно хранится. Оператору фискальных данных, чтобы получить такое разрешение, надо получить кучу лицензий, создать такую систему защиты информации, через которую не проникнет ни один хакер, обучить персонал и еще много чего сделать. Это все стоит денег. И оператору надо эти затраты по крайней мере вернуть. А лишись он разрешения на обработку фискальных данных — его бизнес рухнет, он не сможет окупить свои затраты. И пойти на «слив» информации он, наверное, сможет только в том случае, если ему «заплатят» столько, сколько стоит его бизнес. Не думаю, что конкуренты готовы платить такие деньги... Да и в этом случае начнут действовать репрессивные механизмы, заложенные в законе о ККТ. Попросту говоря, оператору грозит уголовная и административная ответственность.

О персональных данных. На чеке действительно есть должность и фамилия лица, осуществившего расчет с покупателем, что вполне подходит под определение персональных данных со всеми



Не будем забывать, что одним из условий получения разрешения на обработку фискальных данных является наличие у оператора фискальных данных надежной системы защиты информации

вытекающими отсюда последствиями. Но это те персональные данные индивидуального предпринимателя, которые указаны в государственном Реестре регистрации юридических лиц (индивидуальных предпринимателей). А эти сведения сами по себе, в силу закона, являются общедоступными и защищаются только с точки зрения обеспечения их целостности и доступности. Еще одна категория — это фамилия кассира, осуществившего транзакцию. Но включение этой информации в чек — требование закона о ККТ и, в силу этого, является общедоступной. Не нравится это тому, кто хочет стать кассиром — его право отказаться от этой работы.

Не будем забывать, что одним из условий получения разрешения на обработку фискальных данных является наличие у оператора фискальных данных надежной системы защиты информации. Это как раз и обеспечивает защиту и персональных данных, и коммерческой тайны налогоплательщика. Кстати, добросовестный оператор фискальных данных обязательно постарается пройти оценку эффективности такой защиты с привлечением независимых уполномоченных экспертов и выложить результаты такой экспертизы на своем сайте. Как правило, свидетельством надежности защиты информации служит Аттестат соответствия требованиям безопасности информации.

Каждая медаль имеет две стороны. И если на аверсе четко прослеживается надпись «Вред», то на реверсе вполне возможно найти надпись «Польза». Так и тут. Закон разрешает оператору фискальных данных проводить с полученными фискальными данными некоторые манипуляции, в частности, обобщать их. Правда делать это можно только с обезличенными фискальными данными, не позволяющими их соотнести с тем или иным налогоплательщиком. Зато сам налогоплательщик через свой личный кабинет может провести практически в режиме on-line определенные маркетинговые исследования, узнать, какая точка лучше торгу-

ет, какие товары пользуются повышенным спросом, какой продавец лучше и достоин поощрения. Это может быть бесценной информацией для развития и улучшения бизнеса. И позволяет это сделать именно накопление фискальных данных в недрах оператора фискальных данных.

СТРАХИ МЫТАРЕЙ

У налоговых органов свои страхи. Самый серьезный среди них — возможность потери фискальной информации, что, естественно, может повлиять на собираемость налогов. По всей вероятности, полностью устранить этот страх невозможно, но свести его к минимуму — можно. Именно для этих целей законом предусматривается достаточно непростая процедура выдачи разрешения на обработку фискальных данных. Практически идет всесторонняя оценка лояльности оператора фискальных данных. Кроме того, ему предписывается строго хранить и защищать налоговую тайну. Ведь, как ни крути, а ответственность за ее разглашение все-таки будет лежать и на налоговых органах. Оператору предписано оценить все угрозы, сверить их с той моделью, которую разработала ФНС России, применять только разрешенные средства защи-

ты информации, обеспечить бесперебойность работы. И ко всему прочему в законах закладываются серьезные репрессивные механизмы. Не зря введение нового закона о ККТ потребовало значительного изменения и Кодекса об административных нарушениях. Ну и не будем забывать про статью 313 Налогового кодекса, которая относит содержание данных налогового учета (в том числе данных первичных документов) к налоговой тайне. При этом, лица, получившие доступ к информации, содержащейся в данных налогового учета, обязаны хранить налоговую тайну, а за ее разглашение они несут ответственность, установленную действующим законодательством.

С другой стороны, налоговые органы получают уникальную возможность мониторить в реальном времени потоки транзакций и отслеживать все аномалии, которые могут повлиять на собираемость налогов. А чем больше будет собрано налогов, тем лучше и государству, и нам с вами, потому что они, надеюсь, обернутся благами для нас. Вот на этой позитивной ноте я и закончу свое повествование...

Александр БОДРИК

сертифицированный специалист
по управлению информационной
безопасностью корпоративных и облачных
ландшафтов, член ISACA, ASIS, ACFE

ПООХОТИМСЯ... НА «ЧЕРНЫХ ЛЕБЕДЕЙ»!

Как подготовиться к непредсказуемому или Стратегия штанги в кибербезопасности

В последние пару лет стал популярным термин «черный лебедь». Термин обозначает редкие непредсказуемые события со значительными последствиями (начала мировых войн, финансовые кризисы и т.п.). В кибербезопасности таким событием была атака предположительно китайских хакеров на ряд промышленных и высокотехнологичных компаний США (Lockheed Martin, Google и др.), известная как Operation Aurora. По оценке Brookings Institute, атака привела к увеличению стоимости реализуемой Lockheed Martin программы многоцелевого истребителя (Joint Strike Fighter) на 50% (до 388 миллиардов долларов).

Создавая «черных лебедей» в кибербезопасности, злоумышленники используют ранее неизвестные уязвимости (zero day), человеческий фактор (spear phishing), атакуют резервные копии (взлом Hacking Team) и реализуют DDoS атаки мощностью в 470 гигабит (недавно обнаруженная Imperva — атака на китайскую gambling компанию).

Увы, многие из этих проблем практически неразрешимы. К примеру, нельзя на 100% быть уверенными в отсутствии уязвимостей в ПО или довести до идеальной осведомленности пользователей (всегда кто-то будет расстроен, болен или невнимателен). Индустрия кибербезопасности более-менее научилась бороться с известными практиками атак (known evil), но во многом неэффективна перед неизвестными (unknown evil).

Именно на unknown evil направлены десятки и сотни бурно развивающихся

стартапов, именно на них сделали свои миллиардные капитализации Palo Alto и FireEye, но проблема до сих пор не решена. Во многом из-за непонимания руководством организаций необходимости инвестиций.

Со стороны руководства кибербезопасность напоминает «черную дыру», которая с каждым годом все поглощает, ничего не давая взамен. Не дает ни дохода, ни прибыли, ни сколько-нибудь значимой уверенности в устойчивом функционировании бизнеса в информационной сфере. А значит, ситуация аналогична фондовым рынкам, инвестиции в которые автор концепции «черного лебедя» Нассим Талеб сравнивает с игрой в рулетку.

Для повышения возврата на инвестированный в кибербезопасность капитал предлагаю воспользоваться предложенной Талебом стратегией штанги.

Стратегия штанги подразумевает инвестиции в два класса активов:

1. Надежные мало доходные активы (депозиты, государственные облигации и т.п.).

2. Венчурные высокорисковые активы, потенциально приносящие прибыль в сотни и тысячи процентов.

По мнению Талеба, такой портфель позволяет придать антихрупкость (устойчивость к значимым потрясениям) капиталу инвестора. В самом деле, разделяя инвестиции в пропорции 80

на 20 (надежные и высокорисковые инвестиции), мы повторяем старую добрую концепцию структурных продуктов, где инвестор как минимум ничего не потеряет.

Применяя Стратегию штанги в кибербезопасности, менеджмент организации ровно так же инвестирует в надежные проверенные меры (антивирус, управление обновлениями, межсетевой экран, резервное копирование, обучение пользователей) и новейшие практики (геймификация обучения пользователей, поведенческий анализ — UBA, анализ поведения файлов — «песочницы», кластерный анализ трафика в сети и др.).

Стратегия штанги в кибербезопасности отвечает одновременно на вызовы Known и Unknown evil, но потребует изрядной смелости, ведь времени и финансовых ресурсов на привычные многим экспертам по кибербезопасности практики не останется. Могут уйти IDS, сетевое сегментирование, частные политики безопасности — все то, что находится между «гигиеническим минимумом» (надежными средствами) и новейшими практиками.

* * *

Выбирая те или иные меры безопасности, стоит учесть не только потенциальный возврат капитала, но и способность организации их эксплуатировать. Будет сложно получить какой-либо заметный возврат от технологии типа «собери сам» без выделенного для нее квалифицированного специалиста. С другой стороны, при наличии возможности найма высококлассного специалиста, технологии-конструкторы помогут быстрее адаптироваться к запросам стремительно меняющейся действительности.

**Стратегия штанги в кибербезопасности
отвечает одновременно на вызовы
Known и Unknown evil, но потребует
изрядной смелости**

ПРИЗРАК РУССКОГО ХАКЕРА В ЛОНДОНЕ

Proof of address. Пропуска есть?

Открыть сейчас в центральном Лондоне личный текущий счет в крупном первоклассном банке стало большой проблемой, причем, не только для приезжих, но и для коренных англичан. Банки стали ожесточенно бороться с отмывкой денег, истово охраняя свою информационную безопасность. У нас это малоизвестно: россияне наивно верят в то, что, приехав в Лондон, они там запросто откроют банковский счет, как у себя на родине.

Крупнейшие и первоклассные британские банки, расположенные в центральном Лондоне и работающие с физическими лицами, можно пересчитать по пальцам: HSBS, Royal Bank of Scotland, Barclays, Lloyds TSB, National Westminster, Santander и др. Иметь там личный счет удобно и престижно — это своего рода визитная карточка владельца счета.

Наряду с удостоверением личности (паспорт, водительские права и т.д.), при открытии личного текущего счета главным документом клиента для банка является «proof of address» — «подтверждение адреса». Он может включать присланные на домашний адрес выписки банковского счета, счета за оплату коммунальных услуг, извещения из госучреждений, пенсионного фонда и др. Ничего подобного российская банковская система не ведает! Последнее нововведение: лондонские банки стали требовать для открытия сче-



та аж два различных «подтверждения адреса». Одного теперь мало.

Принципиально важно: банки не принимают в качестве «подтверждения адреса» договоры аренды жилья, также письма из медицинских и страховых учреждений. Почему — тайна сия велика есть. Единственное толковое объяснение — эти документы проще всего подделать. Хотя и другие «подтверждения» умельцы подделывают в Лондоне с поистине «одесским» размахом. Уж не знаю...

В результате в банках возникают самые драматические сцены, чему я неоднократно был свидетелем. Новоиспеченные лондонцы разных каст и стран и гости британской столицы уверенно предъявляют договоры аренды жилья, а сотрудники банков с ледяной вежливостью посылают их на все четыре стороны.

Возникает замкнутый круг: для открытия банковского счета необходимо предъявить «подтверждение адреса», а чтобы получить это самое «подтверждение», требуется иметь банковский счет. Такая вот житейская «диалектика».

К слову, «подтверждение адреса» стало в Лондоне своего рода фетишем (как в СССР прописка во времена «культу личности»), без него с тобой в солидном учреждении и разговаривать не станут. Даже для того, чтобы записаться в Национальную библиотеку, требуется предъявить целых два «подтверждения адреса»! Поэтому разговоры бри-

Россияне наивно верят в то, что, приехав в Лондон, они там запросто откроют банковский счет, как у себя на родине

танских политиков о «правах человека» звучат при записи в библиотеку как пустопорожняя болтовня.

Естественно, лондонские банки недополучают большие деньги от несостоявшихся клиентов. Но честь мундира и информационная безопасность для них дороже. Судя по всему, британские банкиры руководствуются ветхозаветным католическим постулатом: «Пусть лучше десять праведников попадут в ад, чем один грешник в рай».

Речь идет, конечно, о простых тружениках, а не об очень богатых индивидуумах любой национальности, сиречь толстосумах, — для них-то в Соединенном Королевстве гостеприимно открыты все двери, включая банковские.

Возникает вопрос: как же трудовые лондонцы и приезжие выходят из этого положения? Да, кто как... Терпеливо ждут пару-тройку месяцев, когда на новый адрес по почте придет «подтверждение», за ним другое. Пользуются услугами отделений банков, расположенных, как говорят коренные лондонцы, «за четвертой зоной» (транспортная сеть города разделена на расходящиеся от центра зоны, за четвертой начинается далекое «подлондонье»), — сотрудники там не столь щепетильны.

Открывают счета в средних и небольших коммерческих банках (в стране их сотни), строительных и страховых компаниях. Активно используют банковские услуги знаменитой Королевской почты. Просят работодателей похлопотать за них перед первоклассным банком, что действует, и т.д. и т.п.

Для россиянина все это странно и непонятно. Нашим банкирам, как говорится, «до лампочки», кто ты такой, где раздобыл деньги на вклад, — заработал их непосильными трудами или зарезал и обчистил кого ночью тёмною.

В первоклассных лондонских банках обычных россиян, жаждущих открыть личный текущий счет, откровенно пугаются. Стена недоверия к нашей стране, выстроенная британскими СМИ, сыграла свою роль. Тень гениального и ужасного российского хакера висит над британскими банками!

* * *

Думается, читателю, замыслившему деловую поездку в Лондон, резонно все это принять во внимание. И не питать иллюзий относительно многовековой британской «демократии», включая банковскую сферу.



ПОЛЕТАЕМ?

- А если у кого-то парашют не раскроется?!!!
- Укладчик парашютов не получит премию...

Итак, на волне кризиса бизнес принимает решение о частичном совмещении функций служб информационной безопасности и экономической безопасности, оставляя частично одних и увольняя частично других. Проводя аналогию ИБ с укладкой парашютов (работа без очевидных результатов при отсутствии ЧП) — укладчикам парашютов вменили в обязанность в свободное от парашютов время укладывать асфальт (работа с понятным всем результатом).

Через какое-то время очень-очень высокое начальство высказало резкое недовольство качеством и темпами укладки асфальта. Пришлось виновников уволить и набрать новых. И вот бизнесу в лице шефа, хочешь — не хочешь, пришла пора прыгать с парашютом. Вызывает шеф главного по кадрам:

- У нас кто парашюты укладывает?
- Укладчики асфальта.
- И что, им можно доверять?
- Асфальт укладывают как боги, а парашюты — дело наживное...

Автор: Валерий Естехин

ДНЕВНИК КУЛХАЦКЕРА

Сегодня впервые взломал компьютер в Интернете! IP адрес: 127.0.0.1. Я крут!.. Вот у кого-то крутой красивый номерок!

После тщательного наблюдения я, наконец, понял: у большинства пользователей пароль состоит из 5–8 звездочек!

Встретил на секретном форуме легендарного хакера! Он сказал, что взломал Интернет и, если я переishу ему 50 баксов, он откроет мне секрет раньше других... Ушел сдавать бутылки...

Одного хакера взяли в США. Сначала грозило 25 лет, но потом он получил всего год, потому что умело заметал следы и никого не сдал из наших...

Написал сегодня письмо в лабораторию Касперского: «Включите в свою базу запись с моим ником. Я вирус писать не буду, просто хочу войти в историю, оставить след!»

Зарегистрировался сегодня на крутом анонимайзере! Работает отлично и супербыстро: уведомление о регистрации сразу пришло мне на почту!

Сегодня я отловил самого матерого хакера-ИБэшника-гуру... Говорю ему: «О великий, научи хакерить и ИБ!!!», а он отвечает: «Не-е, я больше по бабам и пиву...»

Сегодня один авторитетный хакер написал, что первым взломал алфавит... Вот debil, совсем спился и крыша поехала, а я был о нем другого мнения...

Автор: Евгений Родыгин

СКАЗКИ-МАЛЫШКИ

В одной агронефтегазовой стране Чехова не читали, инженеров не кормили и мечтали о зрелой отрасли ИБ... Там и жил-был Один мальчик...

Один мальчик все время твердил, что подразделение ИБ — самый ценный актив компании. Когда случился кризис, его сократили в первую очередь...

Один мальчик решил обеспечить безопасность компании. Посчитал активы, обосновал риски, вывел KPI, нарисовал красивую презентацию, убедил начальника, выбил бюджет, закупил лицензий, и даже нашел подрядчиков... Но вдруг его уволили. Потому что гендиректор потерял в бане свой iPhone с конфиденциальной перепиской.

Один мальчик решил обмануть DLP и заработать у конкурента... Теперь он меняет ФИО и мечтает работать на конкурента, даже не по специальности...

Один мальчик решил пропустить плановый Backup... Теперь он боится пропустить физиотерапию и прием лекарств...

Один мальчик выполнял все требования политики информационной безопасности компании... Ни на что другое времени у него не оставалось...

Один мальчик решил вычитать все презентации Алексея Лукацкого... Но не смог, состарился и умер...

Один мальчик решил провести оценку рисков в своей компании... Через полгода пришел к выводу, что лучше бы он антивирусы дальше настраивал...

Один мальчик придумал перевести активы компании в облака, посчитал TCO, ROI, доказал безопасность... После этого он стал не нужен и его сократили...

В одной большой-пребольшой, богатой и процветающей компании не было ИБ'шника... Так вот... там... у них... все умерли...

Автор: Евгений Родыгин



Каталог решений и услуг по информационной безопасности

Каталог решений и услуг — бесплатная общедоступная отраслевая площадка, где:

- ▶ **поставщики** эффективно доносят до потребителей сведения о своих разработках и услугах
- ▶ **потребители** в удобном виде знакомятся с решениями и услугами по защите информации и делают правильный выбор

Преимущества каталога



информация классифицирована по решениям и услугам, а не по компаниям-разработчикам и продавцам, как это делается на имеющихся сайтах, где каждый продвигает свои товары



информация всегда актуальна (поставщик может без труда поддерживать её в таком состоянии, если, конечно, заинтересован в продвижении своего продукта)



информация не ограничена по объему и может содержать ссылки на любые ресурсы в интернете, связанные с предлагаемым решением

**Бесплатная регистрация
и размещение информации:
catalog.ib-bank.ru**





IX УРАЛЬСКИЙ ФОРУМ

13–17 февраля 2017 года



Ещё больше
участников



Все регуляторы
отрасли



Главный ИБ-форум
финансовой сферы



Лучшие спикеры
отрасли



Настоящая русская
зима

Регистрация открыта:

ural.ib-bank.ru